CLOUD FORENSICS PADA APLIKASI DROPBOX DENGAN METODE NIST (STUDI KASUS : PEMANFAATAN DROPBOX SEBAGAI MEDIA PENYEBARAN FILM BAJAKAN)

Disusun Oleh:

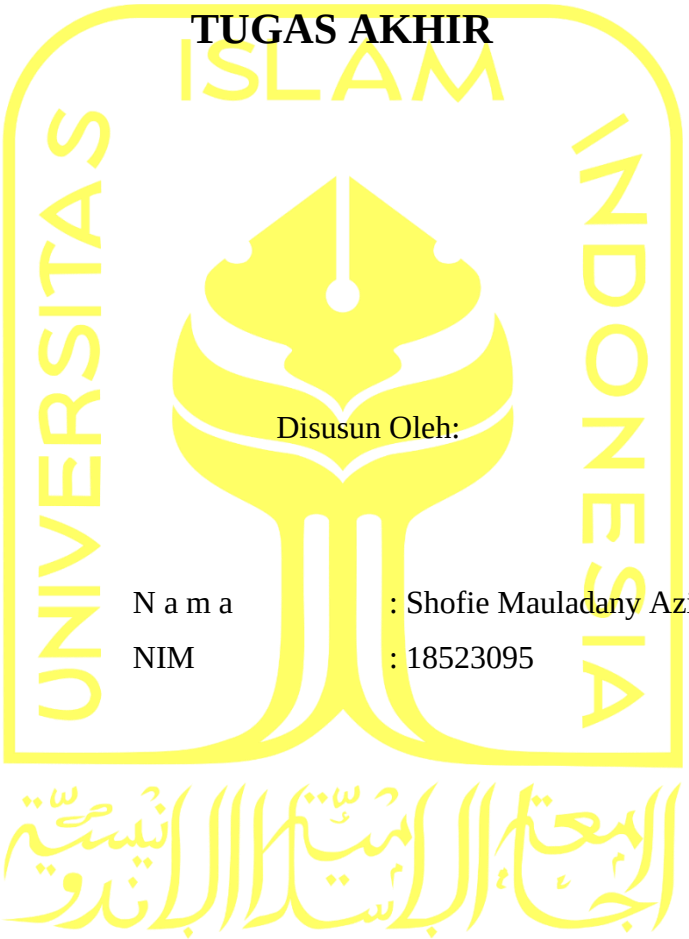
N a m a : Shofie Mauladany Aziz
NIM : 18523095

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ISLAM INDONESIA
2022

HALAMAN PENGESAHAN DOSEN PEMBIMBING

CLOUD FORENSICS PADA APLIKASI DROPBOX DENGAN METODE NIST (STUDI KASUS : PEMANFAATAN DROPBOX SEBAGAI MEDIA PENYEBARAN FILM BAJAKAN)

TUGAS AKHIR



Disusun Oleh:

N a m a	: Shofie Mauladany Aziz
NIM	: 18523095

Yogyakarta, 9 Nopember 2022

Pembimbing,

(Erika Ramadhani S.T., M.Eng.)

HALAMAN PENGESAHAN DOSEN PENGUJI

CLOUD FORENSICS PADA APLIKASI DROPBOX DENGAN METODE NIST (STUDI KASUS : PEMANFAATAN DROPBOX SEBAGAI MEDIA PENYEBARAN FILM BAJAKAN)

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 4 Januari 2023

Tim Penguji

Erika Ramadhani S.T., M.Eng. _____

Anggota 1

Irving Vitra Paputungan, S.T., M.Sc., Ph.D. _____

Anggota 2

Rahadian Kurniawan, S.Kom., M.Kom. _____

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dhomas Hatta Fudholi, S.T., M.Eng, Ph.D)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan di bawah ini:

Nama	:	Shofie Mauladany Aziz
NIM	:	18523095

Tugas akhir dengan judul:

CLOUD FORENSICS PADA APLIKASI DROPBOX DENGAN METODE NIST (STUDI KASUS : PEMANFAATAN DROPBOX SEBAGAI MEDIA PENYEBARAN FILM BAJAKAN)

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 4 Januari 2023

(Shofie Mauladany Aziz)

HALAMAN PERSEMBAHAN

Assalamualaikum Warahmatullahi Wabarakatuh, puji syukur kehadirat Allah SWT yang telah memberikan banyak nikmat sehingga penulisan skripsi ini dapat diselesaikan dengan baik. Skripsi ini dipersembahkan untuk :

1. Alm. Bapak Muazis dan Ibu Siti Aisah selaku kedua orang tua
2. Mas Afien, Syauqie, Syahdan selaku saudara kandung saya
3. Keluarga besar Kos Griya Tentrem
4. Komunitas Cloud Of Dreams
5. Komunitas House Of Maidens

Demikian persembahan ini disampaikan, Wassalamualaikum Warahmatullahi Wabarakatuh.

HALAMAN MOTO

“Berbuat baiklah sesuai kemampuan”

“Menunda pekerjaan adalah salah satu hal yang paling buruk dalam kehidupan”

“Sesibuk apapun dirimu jangan sampai meninggalkan kewajiban ibadah (Sholat)”.

KATA PENGANTAR

Segala puji bagi Tuhan Yang Maha Esa yang telah memberikan nikmat dan karunianya sehingga penulisan skripsi ini telah selesai disusun. Penulisan skripsi ini selesai berkat do'a dan ridho dari kedua orang tua sehingga skripsi ini selesai disusun selama kurang lebih 1 ½ tahun. Berkat dukungan keluarga besar dan juga kerabat semakin terdorong untuk selalu tetap semangat dalam pengerjaan skripsi.

Ucapan terima kasih kepada Mamah, Mas Afien selaku keluarga yang selalu memberikan dukungan jasmani maupun rohani, Ibu Dosen Pembimbing Bu Erika yang senantiasa membimbing saya dengan baik sehingga bisa sampai pada titik ini, serta kepada teman-teman saya Rizky Parindra, Izzan, Irpan, Riza, Greg, Peter, yang selalu memberikan semangat disaat kondisi sedang menurun serta memberikan dukungan penuh pada penulisan skripsi ini. Kendala dalam penulisan skripsi hanya satu yaitu malas, saat malas sudah menguasai maka segalanya akan tertunda, tetapi berkat dukungan kerabat dekat, keluarga dan dosen pembimbing saya berhasil melawan rasa malas itu.

Tujuan penulisan skripsi ini adalah untuk mengetahui bagaimana alur pada cloud forensik aplikasi Dropbox dan juga memberikan informasi terkait pembajakan film yang pada saat ini masih terjadi.

Harapan saya terhadap skripsi ini yaitu ilmu yang disampaikan dapat diterima dengan mudah dan dapat dijadikan contoh untuk penelitian selanjutnya, Sekian Terima kasih.

Yogyakarta, 9 Nopember 2022

(Shofie Mauladany Aziz)

SARI

Kasus pembajakan film seringkali ditemukan terutama di Indonesia mengalami kerugian yang cukup besar akibat pembajakan film. Penyebaran film bajakan dalam bentuk *share link* yang berasal dari *cloud storage* menjadi salah satu kunci diangkatnya topik ini. Dengan metode NIST dalam proses forensik *cloud* menghasilkan pengambilan data yang baik dengan tahapan *Collection*, *Examination*, *Analysis*, dan *Reporting.* Temuan berupa nilai hash pada file database yang terdapat pada aplikasi Dropbox serta mendapatkan nilai hash film bajakan yang tersimpan pada Dropbox.

Kata kunci: forensic, cloud, NIST, Bajak film.

GLOSARIUM

Glosarium memuat daftar kata tertentu yang digunakan dalam laporan dan membutuhkan penjelasan, misalnya kata serapan yang belum lazim digunakan.

cyberbullying	Perundungan pada dunia maya
cloud	awan
crack app	Aplikasi bajakan
NIST	Metode Forensik *National Institute of Standard and Technology*
Path file	lokasi file
streaming	Menonton video menggunakan internet

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Forensik digital umumnya merupakan disiplin ilmu hukum dimana bukti hukum ditemukan pada komputer dan media penyimpanan digital, baik yang berbasis fisik maupun cloud. Forensik digital dapat diartikan sebagai penggunaan teknologi untuk kepentingan hukum dan keadilan. Proses investigasi kasus kriminal, pengamatan dalam bentuk digital dan fisik. Pada dasarnya forensik komputer diperlukan di era digital ini karena teknologi terus berkembang sehingga banyak kasus kriminal yang melibatkan penggunaan teknologi. Menurut Joshua (2020) Digital Forensic Computer Security (IT Security) merupakan kajian menarik yang menerapkan metode tertentu untuk secara ilmiah dan legal menelusuri bukti yang bertanggung jawab untuk mendeteksi suatu kasus kejahatan/kriminal.

Pemanfaatan cloud storage sebagai media penyambung dalam tindak kejahatan kerap terjadi salah satunya penyebaran film bajakan. Pembajakan film adalah suatu tindak kejahatan yang sangat merugikan bagi produser film karena pembajakan film sejatinya adalah tindak pencurian suatu karya. Menurut Undang-Undang Dasar No 28 Tahun 2014 tentang Hak Cipta menjelaskan maksud dari hak cipta yang berbunyi : “Hak Cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan”. Pembajakan film ini memanfaatkan cloud storage sebagai media penyebaran yang dapat diakses bebas di internet salah satunya melalui situs film bajakan dalam kasus ini adalah penyimpanan Dropbox. Dropbox adalah media penyimpanan cloud yang didirikan pada tahun 2007 oleh Drew Houston bersama rekannya Arash Ferdowsi. Tujuan dibuatnya aplikasi Dropbox adalah untuk memudahkan dalam menyimpan berbagai jenis file digital yang dapat diakses melalui Internet. Dropbox memiliki beberapa versi aplikasi, termasuk Android, iOS, Windows, dan MacOS. Versi yang digunakan oleh tema tersebut adalah Dropbox Desktop. Aplikasi Dropbox didesain sangat mudah dipahami terutama bagi pengguna baru karena menyajikan menu yang sangat jelas mulai dari upload dokumen, mencari dokumen yang diupload hingga sharing dokumen.

Gambar 1.1 Kampanye anti pembajakan (APROFI, 2018)

Terutama pada era covid-19 film bajakan sangat diminati karena pada masa pandemi menurut aturan pemerintah seluruh masyarakat tidak diperkenankan untuk keluar rumah demi mengurangi penyebaran virus covid-19 yang membuat seluruh aktivitas pekerjaan dilakukan secara daring.

Pelaku pembajakan dapat dikenakan pidana sesuai dengan pasal 113 Undang-Undang 28 Tahun 2014 tentang Hak Cipta dan pasal 80 Undang-Undang 33 Tahun 2009 tentang Perfilman. Pradesha (2015) menyebutkan bahwa Menkominfo telah memblokir sekiranya 22 situs yang terindikasi pembajakan film karena berdasarkan Peraturan Bersama Menkumham No. 14 tahun 2015 dan Menkominfo No. 26 tahun 2015 tentang Pelaksanaan Penutupan Konten dan atau Hak Akses Pengguna Pelanggaran Hak Cipta dan atau Hak Terkait Dalam Sistem Elektronik. Rochmanudin (2019) Menkominfo memblokir situs bajakan yang sangat terkenal yaitu IndoXXI, dan pada 1 Januari 2020 situs IndoXXI resmi ditutup.

Gambar 1.2 IndoXXI resmi tidak beroperasi (Rochmanudin, 2019)

Judul ini diangkat berdasarkan maraknya pembajakan film yang terjadi terutama di Indonesia, karena pembajakan ini sangat meresahkan bagi industri perfilman yang mengalami kerugian sangat banyak. Murdaningsih (2020) pembajakan film merugikan pihak industri film sebesar 5 Triliun Rupiah tiap tahunnya, pernyataan tersebut dilontarkan oleh ketua umum Asosiasi Produser Film Indonesia (APROFI) Edwin Nazar dan beliau mengatakan bahwa pembajakan sama dengan mencuri. Penelitian ini bertujuan untuk mengetahui bagaimana cara pembajak mendapatkan film tersebut serta berbagai macam penyebaran film bajakan tersebut. Pada dasarnya film merupakan salah satu bentuk dari file digital. File digital dapat dibagikan secara pribadi melalui email dan jaringan pribadi virtual atau dengan memposting ke situs web yang dapat diakses publik seperti YouTube, Instagram, DropBox, atau MediaFire (Hampton-Sosa, 2019). Pengguna masih dapat berbagi konten berhak cipta yang tidak sah dengan kerabat dekat (karena hal itu dapat dilakukan di Dropbox) (Li et al., 2021). Berdasarkan sitasi yang telah disebutkan Dropbox menjadi peluang untuk berbagi konten berhak cipta secara tidak sah dalam kasus ini adalah film bajakan.

Pada artikel ini akan menjelaskan bagaimana cara melakukan analisis forensic pada aplikasi Dropbox berbasis desktop menggunakan metode NIST. Metode NIST adalah metode yang umum digunakan pada analisis forensic. NIST (*National Institute of Standard and*

Technology) merupakan badan nasional non-regulator dari bagian administrasi teknologi Amerika Serikat. NIST sendiri mempunyai langkah-langkah dalam proses forensik. Tahap pertama *Collection*, tahap kedua *Examination*, tahap ketiga *Analysis*, tahap keempat *Reporting* serta menjelaskan bagaimana proses forensik mengenai pemanfaatan Dropbox sebagai media penyebaran film bajakan.

1.2 Batasan Masalah

a. Barang bukti yang diakuisisi berupa nilai hash pada database yang terdapat pada aplikasi Dropbox desktop
b. Studi kasus yang dibahas yaitu film bajakan yang terunggah pada Dropbox.
c. Dropbox yang digunakan versi Desktop

1.3 Rumusan Masalah

a. Bagaimana cara melakukan forensik cloud pada Dropbox menggunakan metode NIST?

1.4 Tujuan Penelitian

a. Dapat mengetahui alur pengerjaan forensik awan menggunakan metode NIST.
b. Mengetahui karakteristik hasil forensik cloud
c. Mencari dan menganalisis cara pembajakan film dan pemanfaatan media Dropbox sebagai alat penyebar film bajakan.

1.5 Manfaat Penelitian

Manfaat yang didapatkan dari penelitian ini adalah dapat mengetahui alur atau proses analisis forensic pada aplikasi Dropbox berbasis desktop menggunakan metode NIST serta mengetahui bagaimana cara pembajakan film bekerja.

1.6 Metodologi Secara Umum

a. Studi Literatur

Pada tahap ini ,dilakukan pencarian referensi tentang metode NIST, cloud forensic, digital forensic, penyimpanan cloud (*cloud storage)* yang kemudian dijadikan bahan acuan pada proses penulisan skripsi.

b. Eksplorasi Data

Pengambilan artefak pada aplikasi Dropbox, pencarian data mengenai pembajakan film, cloud forensic, serta penjelasan mengenai metode yang digunakan.

c. Implementasi

Tahap ini mengimplementasikan metode NIST pada tahap forensik

d. Pengujian

Pada tahap ini pengambilan hasil forensik berupa bukti digital yang dilakukan setelah proses forensik selesai. Proses integrasi file dengan metode berdasarkan pada metode NIST.

e. **Visualisasi data**

Tahap akhir yaitu menyajikan data yang telah diakuisisi dan dianalisis kedalam bentuk tabel. Data tersebut adalah berupa nilai hash sebagai barang bukti yang telah di akuisisi.

1.7 Rancangan Sistematika Penulisan

a. BAB 1 Pendahuluan

Pada bab ini membahas tentang latar belakang penelitian dan juga menjelaskan rumusan, batasan, tujuan, manfaat penelitian.

b. BAB 2 Teori dan Kajian Pustaka

Landasan teori mengenai aplikasi cloud storage Dropbox berbasis desktop dan penelitian terdahulu.

c. BAB 3 Metodologi

Pada bab ini menjelaskan metode NIST yang digunakan sebagai metode forensik serta penjelasan skenario penyebaran film bajakan.

d. BAB 4 Hasil dan Pembahasan

Bab ini berisikan hasil dari penelitian yang telah dilakukan menggunakan metode yang telah dipilih yaitu NIST.

e. BAB 5 Kesimpulan

Bab ini berisikan kesimpulan mengenai penelitian yang telah selesai dilakukan serta saran dari penulis.

BAB II
TEORI DAN KAJIAN PUSTAKA

2.1 Pengertian dan Tujuan Forensik

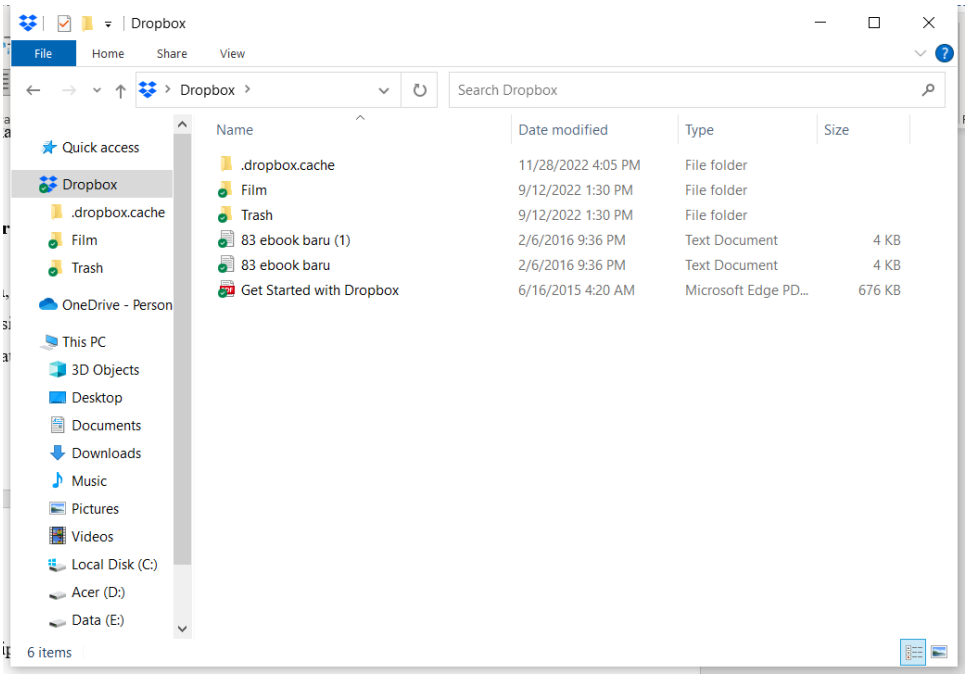
Ilmu forensic adalah ilmu untuk melakukan pemeriksaan dan pengumpulan bukti-bukti fisik yang ditemukan di tempat kejadian perkara dan kemudian dihadirkan di dalam sidang pengadilan (Maramis, 2015). Forensik (berasal dari bahasa Yunani 'Forensis' yang berarti debat atau perdebatan) adalah bidang ilmu pengetahuan yang digunakan untuk membantu proses penegakan keadilan melalui proses penerapan ilmu (sains) (Maramis, 2015). Ilmu forensik sangat membantu aparat penegak hukum untuk mengungkapkan suatu tindak pidana yang terjadi mulai dari tingkat penyidikan sampai pada tahap pengadilan terhadap kasus yang berhubungan dengan tubuh atau jiwa manusia sehingga membuat terang suatu tindak pidana yang terjadi (Romdhoni, 2021). Dalam hal ini menunjukan bahwa peran forensic sangat penting dalam penanganan suatu kasus kejahatan dan juga sangat penting di bidang hukum.

2.2 Dropbox

Dropbox merupakan cloud computing yang sangat favorit karena kemudahannya, dapat diandalkan, mudah diatur konfigurasinya (Saad et al., 2020). Dropbox memiliki berbagai versi aplikasi, yaitu Mobile (Android, iOS), Web, dan Desktop. Dropbox sendiri menyediakan berbagai fitur, salah satu fiturnya adalah ukuran penyimpanan yang disediakan gratis oleh Dropbox kepada pengguna sebesar 2.5 GB(Dropbox, 2022). Untuk versi berbayar Dropbox menyediakan beberapa penawaran mulai dari harga 9.9 USD – 20 USD per bulan dengan beragam kapasitas yang ditawarkan, mulai dari 2 TB hingga tidak terbatas (Dropbox, 2022).

Gambar 2.1 Dropbox (Dropbox, 2017)

Pengguna berbayar, dapat mengamankan file selama maksimal 30 hari. Setelah 30 hari, pengguna tidak dapat mengakses file yang sudah diamankan lebih dari 2.5 GB tersebut apabila belum membayar tagihan pada bulan berikutnya (Dropbox, 2022). Untuk dapat mengakses file tersebut, pengguna cukup membayar tagihan yang telah ditagih.Untuk dropbox versi desktop pada saat ini berbentuk *sync folder* atau terletak pada *file explorer*, terlihat seperti .



Gambar 2.2 Tampilan Dropbox Desktop saat ini

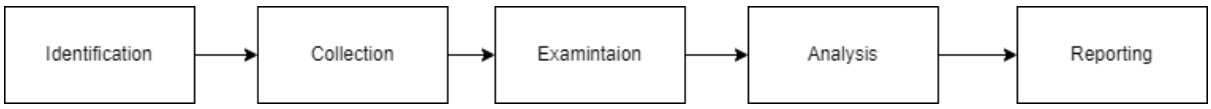
Tampilan seperti ini tentu memudahkan pengguna dalam menggunakan aplikasi karena terhubung langsung dengan *file explorer* pada komputer/laptop. Perbandingan dengan versi sebelumnya Dropbox desktop berbentuk sebuah aplikasi desktop terpisah layaknya aplikasi desktop pada umumnya.

2.3 Metode NIST

Nasirudin et al. (2020) NIST merupakan badan yang bertanggung jawab dalam mengembangkan standar, panduan, dan persyaratan minimum untuk menyediakan keamanan informasi yang cukup bagi semua asset dan pihak-pihak yang memiliki kompetensi di bidang

digital forensic. Lembaga standarisasi teknologi ini memiliki langkah-langkah forensik yang dijadikan acuan terkait analisis forensic yang bertujuan untuk memudahkan para analis melakukan analisis forensic dengan langkah yang mudah dan hasil yang baik. Metode dari NIST biasa digunakan sebagai metode dalam analisis forensik atau pengambilan bukti digital.

Saad et al. (2020) menyebutkan bahwa metode dari National Institute of Standards Technology (NIST) digunakan untuk melakukan tahapan analisis terhadap bukti digital atau tahapan untuk mendapatkan informasi dari bukti digital. Tahapan proses analisis dilakukan sesuai dengan skenario yang telah ditulis. Untuk tahapan pada metode NIST (*National Institute of Standards Technology)* yaitu *Collection, Examination, Analysis, Reporting* (Riadi et al., 2020). Pengambilan barang bukti berupa artefak pada aplikasi Dropbox dan dilakukan pengambilan salinan barang bukti yang dilakukan menggunakan bantuan tool forensik. Setelah diambil, data tersebut diterjemahkan dan dijadikan laporan akhir pada penulisan skripsi ini. Perbedaan metode NIST dengan metode lainnya adalah berada pada tahapan forensiknya, metode selain NIST yang diketahui adalah NIJ *(National Institute of Justice).* NIJ (*National Institute of Justice)* memiliki 5 tahapan, yaitu *Identification, Collection, Examination, Analysis, Reporting* (Riadi et al., 2018). Berikut adalah perbandingan metode NIST dengan metode NIJ.



Gambar 2.3 Metode NIJ

Pada metode NIJ terdapat tahapan *Identification* yang merupakan suatu tahapan yang melakukan identifikasi pada barang bukti untuk menjaga keutuhan barang bukti (Riadi et al., 2018). Pada metode NIST proses identifikasi dilakukan pada tahap *Collection* (Riadi et al., 2020). Kedua metode tersebut memiliki hasil akhir yang sama. Berikut adalah perbandingan metode NIST dengan metode NIJ dalam bentuk tabel.

Tabel 2.1 Perbandingan langkah NIST dengan NIJ

	NIST	NIJ
Tahapan/Langkah	*Collection*	*Identification*
	Examination	*Collection*
	Analysis	*Examination*
	Reporting	*Analysis*
		Reporting

Berdasarkan perbandingan yang telah disebutkan, metode NIST lebih baik digunakan dalam penelitian dibandingkan metode lain karena tahapan yang dilakukan dipersingkat, pada proses identifikasi dan pengumpulan data digabung menjadi satu langkah sehingga memudahkan dalam melakukan analisis forensik.

2.4 Cloud Forensic

Menurut Pichan et al. (2015) cloud forensics dapat didefinisikan sebagai aplikasi forensik digital dalam platform komputasi awan. Pada komputasi awan yang sekarang sangat banyak digunakan, akan menimbulkan suatu masalah baru terkait dengan keamanan daripada komputasi awan itu sendiri. Ilmu forensik Cloud Computing adalah penerapan prinsip prinsip ilmiah, praktik teknologi dan metode turunan dan terbukti untuk memproses peristiwa komputasi awan masa lalu melalui identifikasi, pengumpulan, pelestarian, pemeriksaan, dan pelaporan data digital untuk tujuan memfasilitasi rekonstruksi peristiwa ini. Cloud forensic juga sebagai bagian dari digital forensik yang berkaitan dengan pemulihan bukti digital pada komputasi awan. Cloud forensics dapat dilakukan dengan berbagai metode dan pada setiap metodenya ada resiko masing-masing. Beberapa metode yang biasa dilakukan adalah dengan metode NIST (*National Institute of Standard and Technology),* NIJ (*National Institute of Justice),* dan masih banyak lagi metode yang bisa digunakan.

Pengertian digital forensik menurut Akbar & Kudus (2022) penyelidikan dan analisis komputer untuk menentukan potensi bukti legal. *Computer forensic* dapat diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan.

Menurut Aditya et al. (2021) digital forensik ilmu adalah cabang dari ilmu forensik meliputi pemulihan dan investigasi dari bahan yang ditemukan dalam perangkat digital, seringkali dalam kaitannya dengan kejahatan komputer. Digital Forensik adalah suatu ilmu pengetahuan dan keahlian untuk mengidentifikasi, mengoleksi, menganalisa dan menguji bukti–bukti digital pada saat menangani sebuah kasus yang memerlukan penanganan dan identifikasi barang bukti digital. Proses forensik umumnya meliputi penyitaan, forensic

imaging (akuisisi) dan analisis media digital dan penyusunan laporan berdasarkan bukti yang dikumpulkan.

Barang bukti ini meliputi barang bukti elektronik dan barang bukti digital. Menurut R. A. Ramadhan et al. (2017) Barang bukti elektronik adalah bersifat fisik dan dapat dikenali secara visual (komputer, *handphone, camera, CD, hardisk*, dan lain-lain). Sementara barang bukti digital adalah barang bukti yang diekstrak atau direcover dari barang elektronik (*file, email*, *sms, image, video, log, text*).

2.4.1 Resiko kejahatan

Penggunaan barang digital sudah menjadi kebiasaan sehari-hari dalam melakukan aktivitas pada umumnya. Dalam penggunaan ini terdapat resiko kejahatan yang dapat kita alami, berikut adalah resiko kejahatan digital.

Tabel 2.2 Resiko tindak kejahatan digital

No	Tindak Kejahatan
1	Pencurian data pribadi
2	Penyebaran film bajakan
3	*Cyberbullying*
4	*Phishing*
5	*Ransomware*

(Finance, 2022)

Berdasarkan Tabel 2.2, tindakan kejahatan dapat terjadi dimanapun dan kapanpun, akan tetapi tindakan tersebut dapat diminimalisir dengan adanya suatu pencegahan dini terhadap suatu tindak kejahatan.

Pencurian data pribadi

Berlian (2020) mengatakan pencurian data pribadi sendiri dapat dicegah dengan beberapa langkah yaitu :

a. Mengamankan sandi

Maksud daripada ini adalah kita harus menguatkan kata sandi pada seluruh akun yang kita miliki dengan cara memberikan kata sandi yang tidak ada hubungannya dengan kehidupan kita, dan kita harus membedakan sandi pada semua akun yang kita miliki.

b. **Dilarang membuka tautan yang mencurigakan**

Tanda-tanda yang mencurigakan dari tautan tersebut yaitu tautan yang dikirimkan oleh seseorang yang tidak dikenal, apabila hal itu terjadi pada kita lebih baik diabaikan hal tersebut agar kita terhindar dari phising atau scam dan kita harus memastikan sebelumnya apakah tautan tersebut aman untuk diakses atau tidak.

c. **Membatasi izin privasi**

Aplikasi yang digunakan terkadang membutuhkan izin khusus kepada pengguna agar mendapatkan hak istimewa berupa pengumpulan data pengguna. Data yang dikumpulkan pada umumnya meliputi Riwayat penelusuran, kontak, akses lokasi, dan berbagai sumber data pada perangkat seperti akses penggunaan kamera, *microphone,* dan lain-lain.

d. **Menggunakan Anti-Virus pada perangkat**

Penggunaan anti-virus pada perangkat berguna sebagai pelindung dari sebuah *malware* yang dapat menyerang perangkat. *Malware* tersebut dapat masuk melalui berbagai jalur salah satunya tautan mencurigakan. Pemasangan anti-virus ini dapat mendeteksi hal-hal yang mencurigakan sehingga dapat terhindar dari *malware* tersebut.

e. **Hindari penggunaan aplikasi bajakan**

Aplikasi bajakan atau yang biasa disebut *crack app* merupakan aplikasi yang dapat diakses secara gratis tanpa harus melakukan langganan apabila aplikasi tersebut mengharuskan untuk berlangganan sebelum menggunakan aplikasi tersebut. Aplikasi ini pada umumnya tidak memiliki atau tidak memberikan *update* secara berkala yang dimana merupakan salah satu kesempatan untuk peretas melakukan tindak kejahatannya. Hal ini sangat tidak dibenarkan karena merupakan salah satu bentuk pembajakan pada aplikasi yang merugikan pihak pengembang sehingga dapat dikatakan pencurian.

f. **Pastikan menggunakan koneksi internet yang aman**

Koneksi internet ini sangat sering kita gunakan untuk mengakses berbagai macam hal yang ada pada internet. Tanpa diketahui bahwa jaringan harus kita perhatikan apakah kita sudah menggunakan jaringan yang aman digunakan atau tidak, terutama koneksi wifi. Hal ini sangat diperhatikan karena dengan koneksi jaringan yang tidak aman sangat rentan untuk terkena sadap atau hal yang serupa.

g. **Jangan sembarangan memberikan data pribadi**

Tanpa diketahui apabila kita memberikan data pribadi kepada orang yang tidak dikenal. Data tersebut kemudian akan disalahgunakan yang akan mengakibatkan kerugian pada banyak orang.

Langkah pencegahan yang disebutkan diatas merupakan salah satu langkah pertama yang harus dilakukan agar dapat terhindar dari pencurian data pribadi.

Cyberbullying

Cyberbullying adalah bentuk intimidasi yang pelaku lakukan untuk melecehkan korbannya melalui perangkat teknologi (Pandie & Weismann, 2016). Pelaku ingin melihat seseorang terluka, ada banyak cara yang mereka lakukan untuk menyerang korban dengan pesan kejam dan gambar yang mengganggu dan disebarkan untuk mempermalukan korban bagi orang lain yang melihatnya (Pandie & Weismann, 2016). Menko PMK Muhajir menyebutkan bahwa 45% anak di Indonesia menjadi korban perundungan pada dunia maya atau *cyberbullying* (Utami, 2022).

Gambar 2.4 Ilustrasi *Cyberbullying* (Fisipol, 2022.)

2.5 Penelitian Terdahulu

Penelitian terdahulu digunakan sebagai bahan acuan yang akan digunakan sebagai salah pedoman dalam penulisan skripsi ini. Pencarian literatur dilakukan dengan bantuan *Google Scholar*, dan *Mendeley Desktop.*

Gambar 2.5 Google Scholar (Vectors, 2022)

Gambar 2.6 Mendeley (Team Mendeley, 2012)

Google scholar digunakan untuk mencari literatur yang terkait dengan topik skripsi dengan rentang paling lama 10 tahun kebelakang. Setelah berhasil mendapatkan literatur kemudian ditambahkan ke dalam aplikasi Mendeley agar literatur dapat tersusun rapih. Mendeley juga berfungsi sebagai pengambilan sitasi untuk memberikan sumber pada kutipan yang telah dikutip dari literatur karya orang lain yang ditulis pada skripsi ini. Mendeley juga dapat berfungsi sebagai alat untuk membuat daftar pustaka agar terlihat rapih dan sesuai dengan kaidah penulisan yaitu menggunakan APA style.

Literatur yang ditemukan sebanyak 10 literatur, diantaranya 8 Jurnal Nasional dan 2 Jurnal Internasional. Literatur tersebut dicari menggunakan kata kunci Analisis Forensik dan akan dikategorikan kembali berdasarkan kata kunci yang sesuai pada penulisan skripsi yaitu Analisis Forensik Dropbox. Berikut adalah tabel jurnal yang telah dirangkum.

Tabel 2.3 Penelitian terdahulu terkait Analisis Forensik

NO	TAHUN	PENULIS	BAHASAN	METODE	HASIL
1	2020	(Saad et al., 2020)	Analisis Forensik Aplikasi Dropbox Pada Android	NIST	- Path file pada aplikasi Dropbox mobile terdeteksi mulai dari login sampai akses file - Aktivitas pengguna Dropbox di ponsel

					dapat mudah ditemukan
2	2020	(Nasirudin et al., 2020)	Analisis Forensik Smartphone Android	NIST	- Bukti digital pada smartphone target berhasil ditemukan dengan menggunakan NIST
3	2018	(Syahib et al., 2018)	Analisis Forensik Digital Aplikasi *Beetalk* Untuk Penanganan *Cybercrime*	NIST	- Bukti digital berhasil ditemukan di dalam aplikasi Beetalk.
4	2018	(Yudhana et al., 2018)	Analisis Bukti Digital Facebook Messenger	NIST	- Setelah melakukan proses *rooting* pada ponsel Samsung V+ SMG31HZ, menginstal aplikasi Facebook Messenger, dan investigasi menggunakan tools Oxygen forensic, barang bukti digital ditemukan berupa text percakapan, gambar, dan audio.
5	2021	(Mushlihudin & Nofiyan, 2021)	Analisis Forensik pada Web Phishing	NIST	- Barang bukti berupa IP *address destination*, IP *address server*, DNS pelaku, URL phishing, identitas penyerang dan email yang menghasilkan informasi tindak kejahatan. - Dari semua investigasi telah ditemukan celah untuk mendekripsi HTTPS yang digunakan untuk phishing.

6	2020	(Lim et al., 2020)	Dropbox Forensics: Forensic Analysis of a Cloud Storage Service	Tidak disebutkan	- Menelusuri artefak pada aplikasi Dropbox yang di *install* dengan operasi sistem Windows 10. Penelusuran dilakukan mulai dari tahap proses instalasi hingga menemukan file.db pada aplikasi Dropbox.
7	2019	(Satrya, 2019)	Digital Forensics Study of a Cloud Storage Client: A Dropbox Artifact Analysis	McKemmish Model	- Proses analisis forensik Dropbox dilakukan pada smartphone android. Proses analisis menghasilkan sebuah artefak pada aplikasi Dropbox android yang mencatat semua kegiatan pada aplikasi. Data tersebut berbentuk file.db atau database yang kemudian dianalisis dan ditentukan aktivitas yang dilakukan pada aplikasi berdasarkan file.db tersebut.
8	2020	(Buyu & Abade, 2020)	Forensic Analysis of Dropbox Data Remnants on Windows 10	McKemmish Model	- File database berhasil ditemukan dan dianalisis sehingga dapat mengetahui informasi mengenai file tersebut. Berhasil mendapatkan registry dari Dropbox pada Windows 10, dan dapat menemukan

						perubahan registry yang terjadi akibat pemasangan aplikasi dan pencopotan aplikasi Dropbox.
9	2015	(Ko & Zaw, 2015)	Digital forensic investigation of Dropbox cloud storage service	NIST	-	Dalam penelitian ini penulis berhasil menemukan artefak pada Dropbox berupa file database serta menemukan direktori file Dropbox pada Windows 8.
10	2020	(Lasniroha et al., 2020a)	Mengidentifikasi Artefak Pada Aplikasi Dropbox Untuk Mendukung Forensic Android	NIST	-	Penulis berhasil menemukan artefak pada Dropbox Android berupa file.db yang berisikan aktivitas yang ada pada aplikasi dan mengecek keaslian file tersebut dengan melihat nilai Hash pada masing-masing file db.

Berdasarkan pada Tabel 2.3 terdapat 10 jurnal 2 diantaranya jurnal internasional, dan 8 jurnal nasional. Kemudian literatur akan dikelompokkan kembali berdasarkan tahun terbit literatur. Tahun literatur yang relevan untuk dijadikan referensi sekiranya tidak lebih dari 10 tahun yang lalu sejak penulisan skripsi.

Tabel 2.4 Jumlah Literatur berdasarkan Tahun Terbit

Tahun Terbit	Literatur	Jumlah
2015	9	1
2018	3,4	2
2019	7	1
2020	1,2,6,8,10	5
2021	5	1

Berdasarkan hasil pengelompokan pada Tabel 2.4 tercatat bahwa literatur dengan tahun terbit terbanyak adalah tahun 2020 dengan jumlah 5 literatur, disusul dengan tahun 2018 dengan jumlah 2 literatur, 2015, 2019, 2021 berjumlah 1 literatur. Literatur tersebut kemudian dikelompokkan berdasarkan kata kunci yang sesuai dengan topik pada penulisan skripsi yaitu Forensik Dropbox.

Tabel 2.5 Jumlah Literatur berdasarkan Kata Kunci

Kata Kunci	Literatur	Jumlah Literatur
Analisis Forensik	2,3,4,5	4
Forensik Dropbox	1,6,7,8,9,10	6

Berdasarkan Tabel 2.5 bahwa literatur yang memiliki kata kunci sesuai dengan penulisan skripsi berjumlah 5 literatur. Dari 5 literatur tersebut, memiliki metode yang berbeda-beda diantaranya ada NIST, McKemmish Model, dan ada yang tidak disebutkan metode apa yang digunakan pada literatur tersebut. Metode yang digunakan sebagai acuan untuk penulisan skripsi yaitu metode NIST.

Tabel 2.6 Metode-metode yang digunakan

Metode	Literatur	Jumlah Literatur
NIST	1,9,10	3
McKemmish Model	7,8	2
Tidak disebutkan	6	1

Hasil pengelompokkan literatur sesuai dengan Tabel 2.6 dapat disimpulkan bahwa metode yang paling banyak digunakan yaitu metode NIST. Berdasarkan hasil dari seluruh pengelompokkan pada literatur, pembahasan yang akan dilakukan yaitu literatur yang memiliki kata kunci Analisis Forensik Dropbox yang berjumlah 6 literatur.

2.5.1 Pembahasan Literatur

Buyu & Abade (2020) Pengambilan barang bukti yang dilakukan adalah artefak pada Dropbox versi desktop yang dijalankan menggunakan sistem operasi Windows 10. Penulis menemukan tools yang digunakan : VMWare, Access Data FTK Imager, Regshot, DB Browser for SQLite, GlassWire, HxD, EaseUS Data Recovery Wizard, Autopsy dengan langkah identifikasi artefak pada virtual machine yang dibuat menggunakan VMWare. (Buyu & Abade, 2020a) langkah ini dilakukan mulai dari tahap pemasangan dropbox pada virtual machine, unggah file ke dalam folder dropbox, menghapus file, dan pencopotan aplikasi dropbox pada virtual machine. Buyu & Abade (2020) melakukan penyimpanan barang bukti yang dibantu oleh Access Data FTK Imager yang digunakan untuk membuat salinan VM (virtual machine) yang telah dibuat. Kemudian pengambilan artefak berikutnya yaitu registry pada aplikasi dropbox yang terpasang pada VM (virtual machine). Artefak berikutnya yaitu diambil menggunakan registry yang dapat mengetahui apa saja fungsi yang ada pada aplikasi dropbox. Langkah berikutnya yang dilakukan yaitu pengembalian file yang telah dihapus dengan bantuan tools Autopsy, dan EaseUS Data Recovery Wizard.

Ko & Zaw (2015) menggunakan VMWare dan melakukan pemasangan Windows pada VM (Virtual Machine). Adapun tools yang digunakan yaitu : VMWare, Windows 7, Dropbox Client, Mozilla Firefox 33.0, Google Chrome 38.0, CCleaner 4.19. Pada saat pemasangan Dropbox Client pada VM ditemukan artefak berupa path file pada Dropbox Client mulai dari Install file path, Sync Folder, Default file, Link file, Libraries, Prefetch files, dan Database File. Setelah ditemukannya path file yang menunjukkan dimana lokasi Dropbox Client berada. Penulis menemukan artefak penting yaitu database Dropbox. Ko & Zaw (2015) berhasil menemukan isi dari database tersebut, yaitu Host id, Email pengguna, PC Display Name, Dropbox Path. Database ini dapat menampilkan apa saja yang telah terekam pada database berdasarkan kegiatan yang telah dilakukan. Database dapat dibaca menggunakan tools SQLite yang kemudian dapat menampilkan secara rinci isi dari database tersebut. Database inilah yang kemudian diakuisisi dan dijadikan sebagai barang bukti digital.

Satrya (2019) menggunakan perangkat android dengan tipe Oppo A37 dengan sistem operasi Android Lollipop, dan Samsung A7 dengan sistem operasi Android Nougat. Satrya (2019) menggunakan tools Android Debug Bridge, Busybox Pro v27, VRoot v1.7.3, Dropbox

v150.2.4, SQLite Browser v3.7.0, SQLite v3.8.11. Langkah pertama yang dilakukan yaitu melakukan rooting pada kedua perangkat Oppo A37 dan Samsung A7.Satrya (2019) dalam penjelasannya rooting adalah proses yang memungkinkan pengguna untuk mendapatkan hak kontrol tertinggi, dan rooting itu penting karena ada folder dan data tertentu yang hanya bisa diakses ketika smartphone sudah di root. Analisis yang dilakukan Satrya (2019) meliputi analisis pada instalasi data, sign up data, login data, logout data, uploading data, downloading data, File operation data (Open), File operation data (New Folder), File operation data (New file), File operation data (Move), File operation data (Rename), File operation data (Share), File operation data (Delete), Uninstall data. Seluruh file dianalisis dalam bentuk database. Masing-masing database di identifikasi apa saja informasi yang terdapat pada database tersebut.

Saad et al. (2020) melakukan analisis forensik aplikasi Dropbox pada Android Samsung Galaxy V Plus dan Samsung Galaxy Trend Plus . Adapun tools yang digunakan dalam penelitian yaitu : Android Debug Bridge (ADB), dan Busybox. Pengambilan barang bukti dilakukan dengan cara mencari database yang berisikan kegiatan pada penggunaan aplikasi dropbox pada android. Database tersebut merekam kegiatan mulai dari Install, Sign up, login, logout, Upload, Download, File operation data (Open), File operation data (New Folder), File operation data (New file), File operation data (Move), File operation data (Rename), File operation data (Share), File operation data (Delete), Uninstall data (Saad et al., 2020a). Setelah semua telah terkumpul, dapat disimpulkan pencarian artefak pada Samsung Galaxy Trend dapat dilakukan dengan mudah dengan cara membandingkan direktori dan database yang berasal dari aktivitas-aktivitas tersebut.

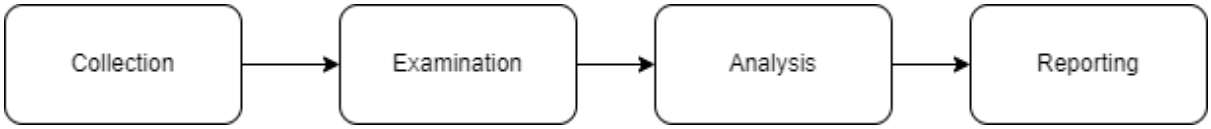
Lim et al. (2020) melakukan pengambilan artefak pada aplikasi Dropbox berbasis desktop yang berupa Registry aplikasi Dropbox, Database, dan Jaringan Aktivitas yang ada pada aplikasi Dropbox. Tools yang digunakan yaitu : Winlogon Registry, Wireshark, CurrPorts, LiveTcpUdpWatch, dan SQLite DB. Langkah pertama yang dilakukan yaitu melakukan pemasangan aplikasi Dropbox pada windows, dan melakukan pengecekan registry dengan bantuan Winlogon Registry. Registry banyak perubahan menarik yang terjadi selama proses instalasi (Lim et al., 2020). Beberapa nilai pendaftar dibuat selama proses instalasi Dropbox. Lim et al. (2020) registry Winlogon adalah komponen sistem operasi Microsoft Windows yang tersedia untuk digunakan di berbagai aplikasi, seperti profil kecil, dan

screensaver komputer (bahasa memori yang dapat diakses) opsional yang dibuat oleh komputer. Kemudian setiap kegiatan yang dilakukan pada aplikasi Dropbox akan membuat suatu registry. Aktivitas jaringan pada saat mengakses Dropbox merupakan bagian dari artefak yang bagus untuk diakuisisi. Aktivitas jaringan dianalisis menggunakan Wireshark dan LiveTcpUdpWatch yang menampilkan IP, Server, Address, serta alamat HTTP yang ada pada Dropbox tersebut. Pengambilan artefak berikutnya yaitu database yang terdapat pada aplikasi Dropbox. Database tersebut berisikan seluruh aktivitas yang telah dilakukan pada aplikasi Dropbox.

Lasniroha et al. (2020) melakukan analisis forensik aplikasi Dropbox pada Android. Perangkat yang digunakan berupa smartphone dengan tipe Xiaomi Redmi 4A (Android 9) (Lasniroha et al., 2020b). Tools yang digunakan yaitu : Dropbox v198.2.2, Resurrection Remix Pie, Root Explorer v4.7.1, dan SQL DB Browser v3.8.0. Langkah pertama yang dilakukan yaitu pemasangan aplikasi Dropbox pada ponsel, kemudian ponsel tersebut dipastikan dalam keadaan telah melakukan proses root. Proses selanjutnya yaitu melakukan aktivitas pada aplikasi dropbox mulai dari Sign In, Sign Out, Download. aktivitas yang telah dilakukan akan membentuk suatu file database yang kemudian akan diperiksa integritas pada file database tersebut menggunakan checksum SHA-1 (Lasniroha et al., 2020).

BAB III
METODOLOGI PENELITIAN

3.1 NIST



Gambar 3.1 Metode NIST

Berikut langkah-langkah dalam metode NIST

a. *Collection* (Pengumpulan data)

Pada tahap ini dilakukan pengumpulan bahan atau data yang mendukung dalam pengambilan serta pencarian bukti digital. Pada tahap ini juga dilakukan pendokumentasian dan preservasi pada bukti digital.

b. *Examination* (Akuisisi data)

Akuisisi data yang dilakukan berupa pengambilan artefak yang terdapat pada aplikasi dropbox serta pengambilan database yang berisikan log atau riwayat aktifitas. Proses ini dibantu menggunakan tools yang sudah disiapkan supaya memudahkan pada saat pengambilan artefak tersebut.

c. *Analysis* (Analisis Data)

Pada tahap ini file .db akan dianalisis dan kemudian dijadikan laporan pada akhir penulisan skripsi ini.

d. *Reporting* (Laporan)

Tahap akhir yaitu pelaporan dari hasil investigasi dan data-data yang diperoleh saat investigasi. Laporan ini berisikan seluruh hasil yang telah ditemukan pada saat proses analisis telah selesai dilakukan.

3.2 Skenario Kejahatan

Skenario yang digunakan pada penulisan skripsi adalah pemanfaatan Dropbox sebagai media penyebaran film bajakan gambaran alur pembajakan terlihat pada Gambar 3.2.

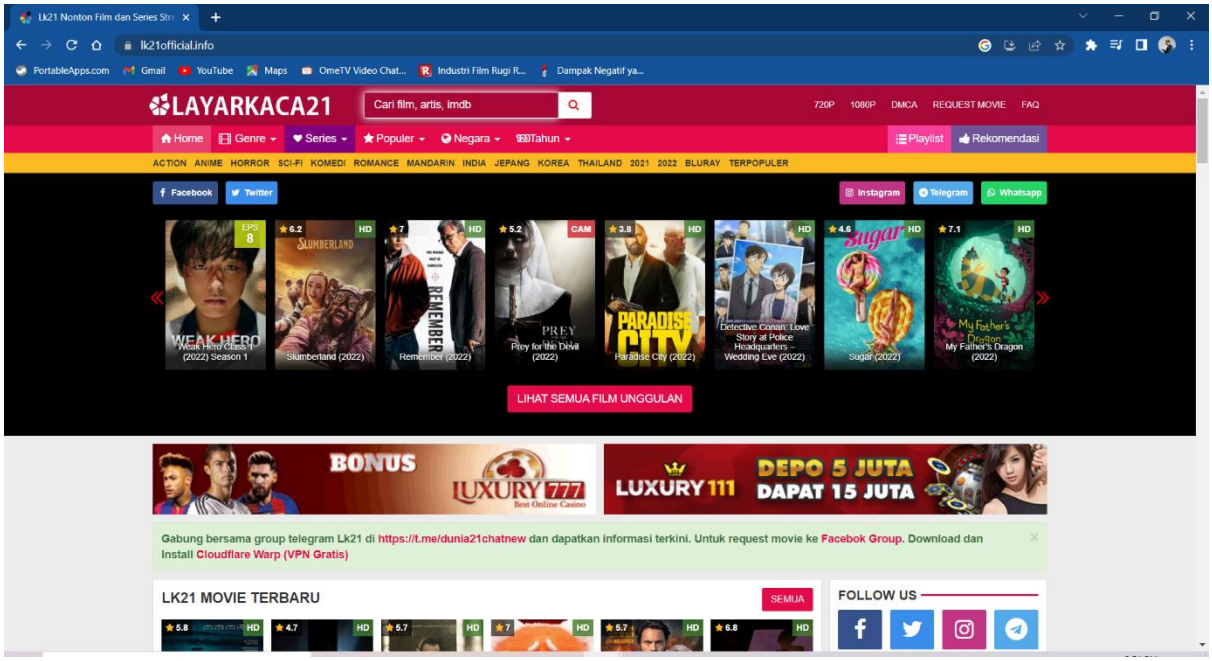
Gambar 3.2 Gambaran skenario pembajak film

Penjelasan pada Gambar 3.2 yaitu alur bagaimana pembajak film melakukan aksi nya yang dimulai dari pembajak melakukan pencurian terhadap file rahasia yang dimiliki oleh bioskop dan kemudian setelah mendapatkan film tersebut diunggah ke penyimpanan cloud setelah selesai mengunggah kemudian para pembajak membuatkan situs yang didalam situsnya berisikan banyak film yang telah dicuri atau dibajak dan kemudian situs tersebut disebarluaskan ke seluruh masyarakat melalui internet yang dapat diakses oleh siapapun yang terhubung internet.

Pembajakan ini memanfaatkan salah satunya cloud storage sebagai media penyimpanan film yang disebarluaskan melalui situs bajakan, *link share,* dan masih banyak lagi. Berawal dari pengunduhan film yang tersedia pada situs film illegal atau bajakan yang kemudian diunggah ke dalam *cloud storage* dan disebaarluaskan melalui internet. Hal tersebut termasuk salah satu dari bentuk pembajakan film.

3.2.1 Situs Film Bajakan

Penyebaran film bajakan melalui situs tersendiri sangat banyak ditemukan dan sering sekali diakses bagi para penikmat film. Situs ini dibuat oleh para pembajak film dan menjadi alternatif bagi para penikmat film apabila tidak dapat menonton film secara langsung. Banyak sekali situs-situs film bajakan di internet yang dapat diakses bebas salah satunya Lk21 yang terlihat pada Gambar 3.3.



Gambar 3.3 Tangkapan layar pada situs lk21official.info (Aziz, 2022b)

Situs ini memiliki ribuan film dengan berbagai genre dan tahun rilis film. Tahun rilis film yang ada pada situs LK21 mulai dari tahun 1920-2022. Situs ini memiliki cara kerja yang sederhana, pada dasarnya situs ini hanya menempelkan tautan dimana film itu disimpan. Sejatinya situs tersebut tidak memiliki penyimpanan sendiri melainkan memanfaatkan penyimpanan cloud. Pemanfaatan cloud storage ini yang kemudian menjadi media yang membantu dalam proses penyebaran film bajakan. LK21 menjadi salah satunya situs film bajakan yang dapat diakses bebas hingga saat ini, beberapa kali LK21 telah ditutup servernya oleh pemerintah namun dengan segala upaya LK21 membuka kembali dengan mengganti domain.

BAB IV
PEMBAHASAN DAN HASIL

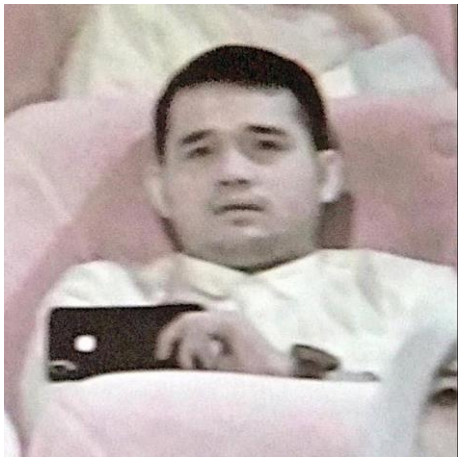
4.1 Pembahasan Skenario

4.1.1 Cara pembajakan film

Pembajakan film dapat dilakukan dengan berbagai cara, adapun cara yang dilakukan mulai dari yang sederhana hingga sulit. Berikut cara pembajak mendapatkan film yang pada akhirnya disebarluaskan melalui situs film bajakan.

a. Merekam di bioskop secara langsung

Tindakan ini sudah ditegaskan bahwa para pengunjung dilarang untuk merekam saat menonton film di bioskop, akan tetapi tetap ada yang melakukan tindakan demikian. Aksi perekaman dilakukan secara tersembunyi sehingga tidak terlihat oleh kamera CCTV yang terdapat pada tiap sudut studio.



Gambar 4.1 Perekam yang tertangkap cctv di bioskop (Putra, 2020)

Apabila tertangkap oleh CCTV maka petugas bioskop akan langsung memberikan teguran berupa menghapus video yang telah direkam di dalam bioskop atau langsung diproses melalui jalur hukum.

b. Pencurian file bioskop

Pencurian secara langsung memerlukan keahlian khusus yang dimana pelaku pembajakan melakukan pencurian film yang berasal dari file rahasia yang dimiliki pihak bioskop. Tindakan ini cukup liar dan jahat karena melakukan pencurian secara langsung. Ramadhan (2021) file digital bioskop dalam bentuk tersebut tersimpan dalam sebuah HDD khusus yang dimana HDD tersebut dapat mencatat siapa dan kapan telah diakses yang seharusnya sangat sulit untuk di bajak.

c. Merekam ulang film pada layanan *streaming* berbayar

Merekam ulang film pada suatu layanan *streaming* berbayar merupakan tindakan yang licik, walaupun tindakan ini terbilang cukup tradisional akan tetapi memberikan dampak buruk bagi pemilik film. Merekam ulang dan kemudian disebarluaskan melalui media sosial yang dimana dapat diakses dengan bebas. Pada media sosial pun terdapat perlindungan hak cipta sehingga apabila mengunggah video yang melanggar hak cipta akan otomatis terhapus, maka dari itu memanfaatkan penyimpanan cloud sebagai media penyambung. Layanan *streaming* berbayar yang tersedia di Indonesia yaitu Netflix, Disney+, dan masih banyak lainnya.

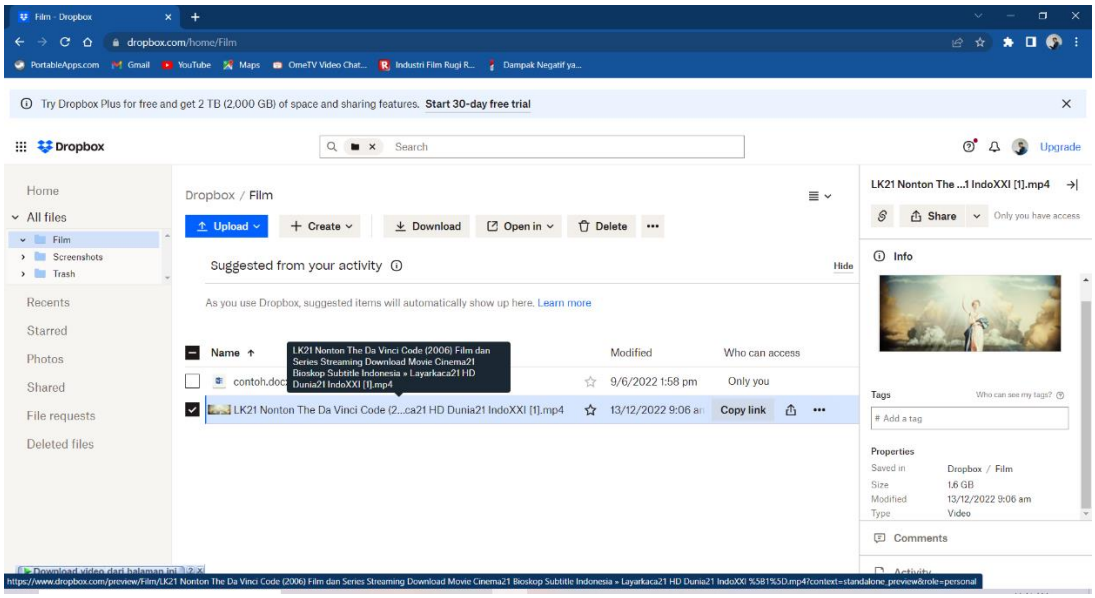
Gambar 4.2 Netflix (Rourke, 2020)

Singkatnya pelaku melakukan pembayaran terkait langganan pada salah satu penyedia layanan *streaming* yang kemudian dapat menonton film yang tidak pernah ditayangkan sebelumnya lalu merekam ulang dan kemudian disebarluaskan agar orang lain dapat melihat juga. Perbuatan ini merupakan penayangan secara ilegal dan pelaku dapat dikenakan undang-undang dan akan mendapatkan hukuman pidana.

4.1.2 Cara Penyebaran Film Bajakan Melalui Dropbox

Gambar 4.3 Gambaran alur penyebaran

Penjelasan pada Gambar 4.3 yaitu penyebar mengambil film melalui situs ilegal dan kemudian mengunggahnya ke penyimpanan cloud setelah berhasil terunggah pelaku membuatkan link tautan lalu menyebarkannya melalui berbagai sosial media yang dapat diakses bebas.Dropbox digunakan sebagai media penyebaran film bajakan melalui fitur berbagi tautan yang dapat diakses seluruh pengguna internet. Dalam penelitian ini pengambilan film bajakan berasal dari salah satu situs film bajakan yang sampai saat ini masih dapat diakses bebas melalui internet yaitu https://lk21official.info/ yang tertera pada Gambar 3.3. Salah satu film yang diambil yaitu film dengan sutradara Ron Howard yang rilis pada tahun 2006 dengan judul The Da Vinci Code. Film tersebut yang kemudian diunduh dan diunggah ke dalam Dropbox.



Gambar 4.4 Film bajakan pada Dropbox (Aziz, 2022a)

Setelah kemudian terunggah, penyebaran film tersebut yaitu melalui fitur *share link* yang terdapat pada tombol “Copy Link” dan akan tersalin tautan film tersebut yang dapat diakses bebas oleh pengguna lain dan disebarluaskan melalui internet salah satunya yaitu sosial media.

4.2 Pengambilan artefak

Proses pengambilan artefak pada aplikasi Dropbox dilakukan untuk keperluan analisis forensic. Proses ini dilakukan berdasarkan metode yang digunakan yaitu NIST.

4.2.1 Collection

Tahap ini melakukan pengumpulan bahan atau *tools* yang akan digunakan untuk proses forensik. Berikut adalah *tools* yang digunakan untuk melakukan proses analisis forensik.

Tabel 4.1 Tools yang digunakan

Tools	Versi
Windows 10	Home Single Language
Access Data FTK Imager	4.5.0.3
Dropbox Desktop	161.4.4923
Magnet Forensics	4.10.0.23663
DB Browser for SQLite	3.12.2

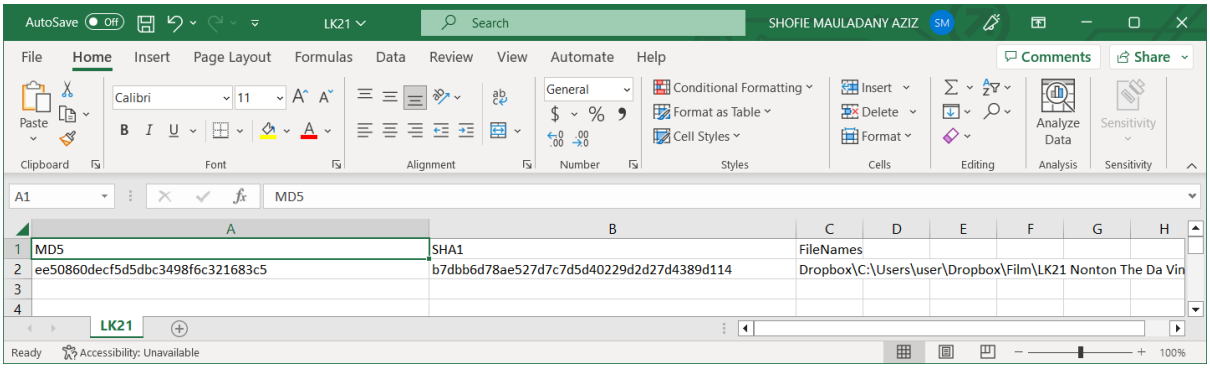
Adapun fungsi dari masing-masing *tools* tertulis dalam Tabel 4.2

Tabel 4.2 Fungsi dari setiap tools

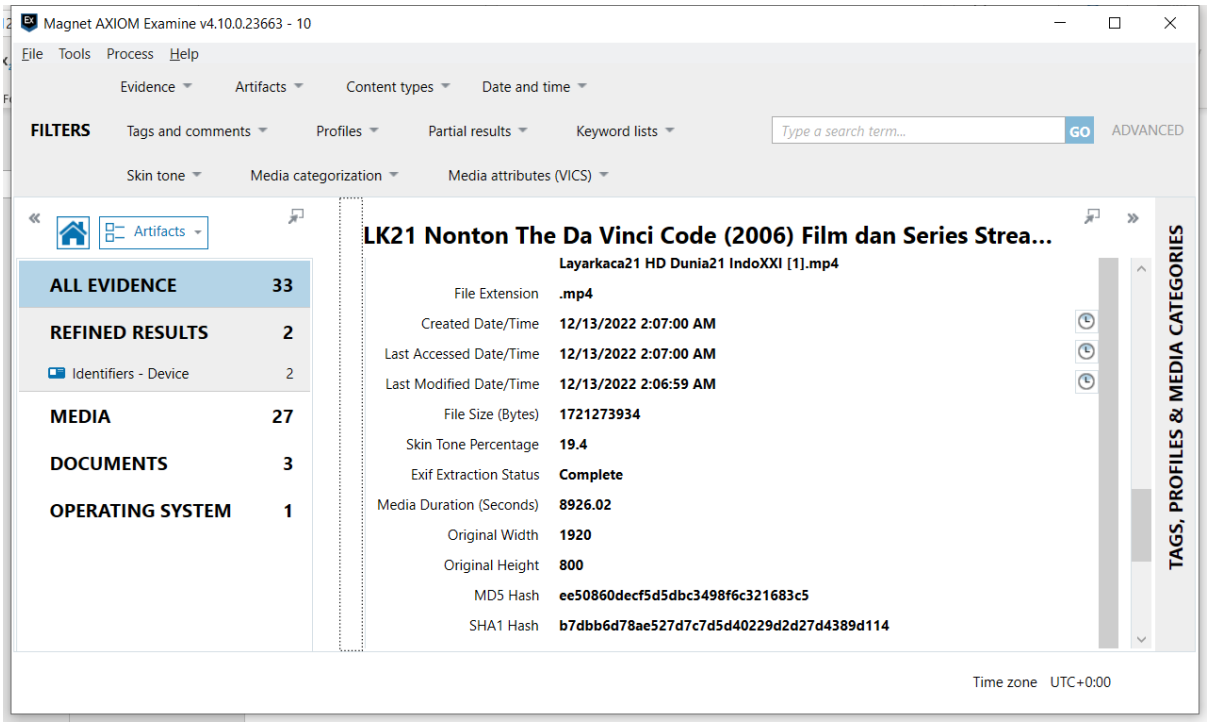
Tools	Fungsi
Windows 10	Sebagai sistem operasi
Access Data FTK Imager	Pengakuisisian barang bukti yang menghasilkan nilai hash pada suatu file.
Dropbox Desktop	Aplikasi yang akan dianalisis
Magnet Forensics	Pengakuisisi barang bukti yang menghasilkan informasi detail mengenai barang bukti
DB Browser for SQLite	Melihat isi dari database

4.2.2 Examination

Pada tahap ini dilakukan proses pengambilan artefak berupa nilai hash pada setiap file yang telah diakuisisi. Pemeriksaan nilai pada setiap file yang telah diakuisisi bertujuan untuk memeriksa dan menjaga keaslian dari setiap file tersebut. Pengecekan nilai Hash dapat dilakukan menggunakan aplikasi FTK Imager dan Magnet Forensic, kedua *tools* tersebut dapat memeriksa nilai hash dan hasil dari kedua tools sama baik, adapun perbandingan antara kedua tools tersebut terlihat pada Gambar 4.5 dan Gambar 4.6. Percobaan menggunakan file film bajakan yang terdapat pada *sync folder* Dropbox.



Gambar 4.5 Nilai Hash oleh FTK Imager



Gambar 4.6 Nilai Hash oleh Magnet Forensics

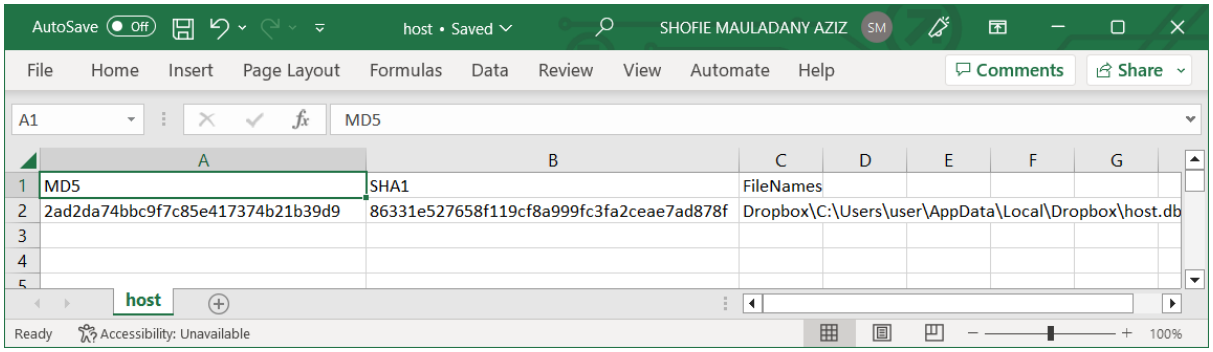
Berdasarkan Gambar 4.5 dan Gambar 4.6 FTK Imager mengeluarkan nilai Hash dalam bentuk file .csv sedangkan Magnet Axiom tertampilkan langsung pada bagian Detail. Dari kedua *tools* tersebut masing-masing memiliki keunggulan yang berbeda yaitu pada FTK Imager kita dapat memeriksa nilai hash dari setiap database yang ada pada Dropbox dan Magnet Forensic tidak dapat melakukan hal demikian, akan tetapi Magnet Forensic dapat menjelaskan secara detail file yang telah diakuisisi mulai dari tanggal akses, tanggal pembuatan, dan lainnya, sedangkan FTK Imager hanya dapat memberikan informasi tentang nilai hash dan path file. Berikut hasil nilai hash yang dihasilkan oleh kedua *tools* tersebut tertulis pada Tabel 4.3.

Tabel 4.3 Nilai hash pada file contoh oleh FTK Imager dan Magnet Forensic

MD5	SHA1
ee50860decf5d5dbc3498f6c321683c5	b7dbb6d78ae527d7c7d5d40229d2d27d4389d114

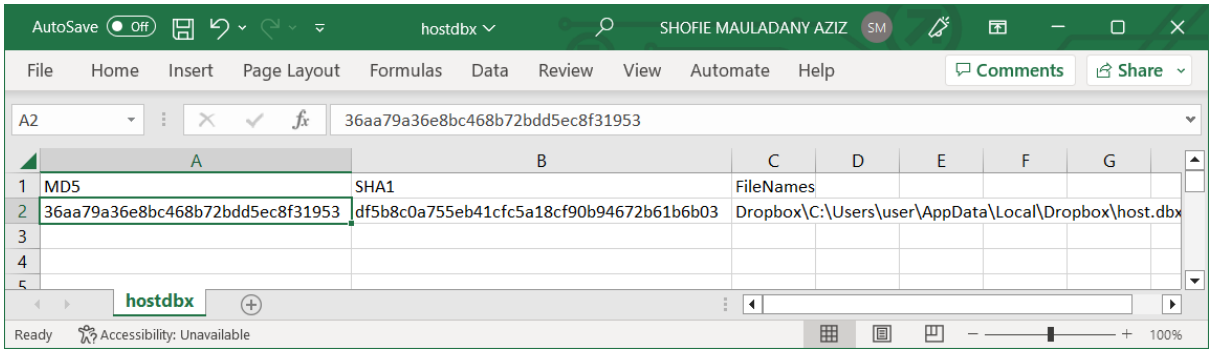
Hash pada database

Pemeriksaan nilai hash pada setiap database dilakukan untuk menjaga keaslian file.db tersebut saat proses akuisisi file.db berhasil dilakukan. Sebelum semua dilakukan harus mengetahui lokasi file.db berada. Folder tersebut telah ditemukan dan akan dilakukan pengecekan terhadap nilai hash setiap database. Database yang di cek merupakan database inti daripada aplikasi Dropbox Desktop. Nilai hash pada tiap database akan ditampilkan dalam bentuk tabel dan dilakukan menggunakan *tools* FTK Imager, sebelum dilakukan pemeriksaan nilai hash pada database yang akan diuji adalah seluruh database yang telah ditemukan pada penelitan ini.



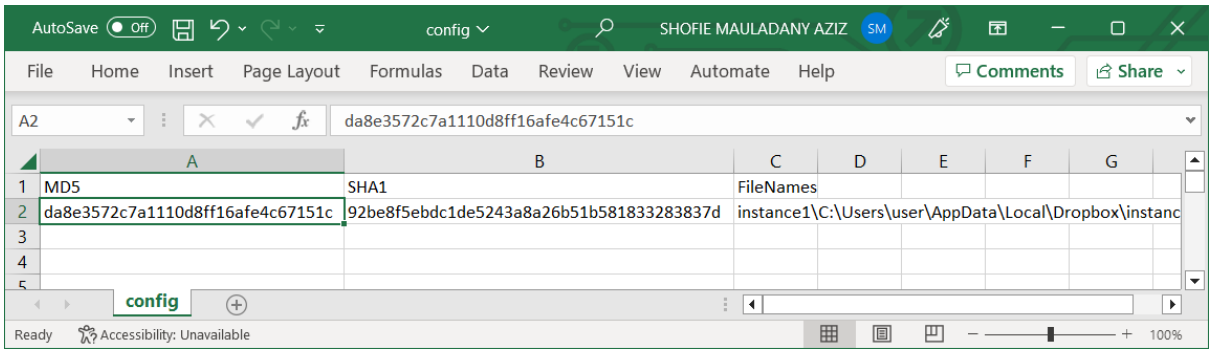
Gambar 4.7 Nilai Hash host.db

Pengecekan nilai hash pada host.db menggunakan *tools* FTK Imager tertampil pada Gambar 4.7 yaitu memiliki nilai MD5 2ad2da74bbc9f7c85e417374b21b39d9 dan nilai SHA1 86331e527658f119cf8a999fc3fa2ceae7ad878f.



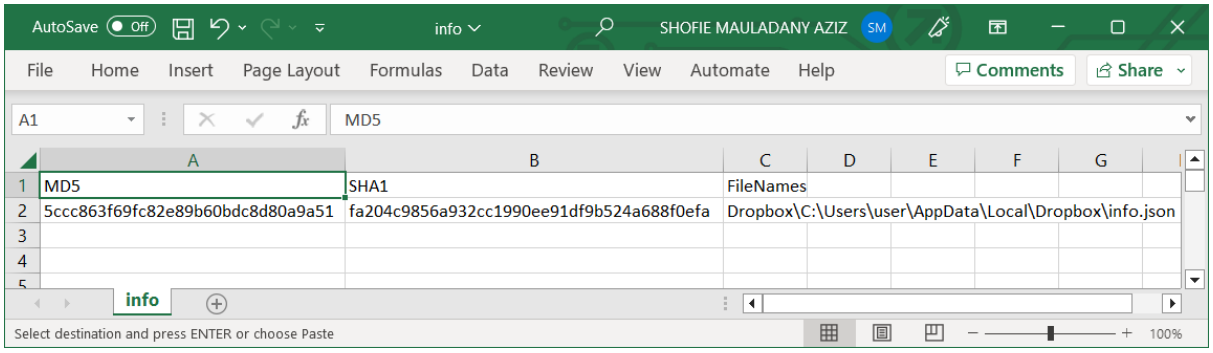
Gambar 4.8 Nilai Hash host.dbx

Pengecekan nilai hash pada host.dbx menggunakan *tools* FTK Imager yang tertampil pada Gambar 4.8 yaitu memiliki nilai MD5 36aa79a36e8bc468b72bdd5ec8f3195 dan nilai SHA1 df5b8c0a755eb41cfc5a18cf90b94672b61b6b03.



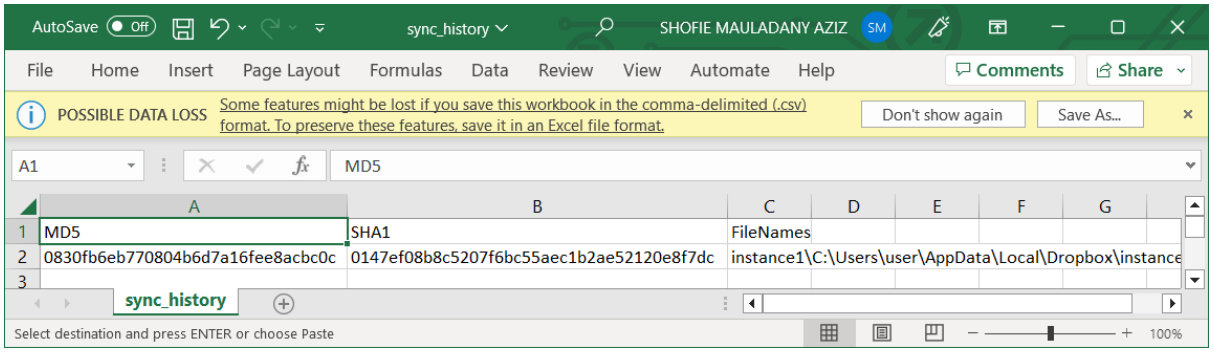
Gambar 4.9 Nilai Hash config.dbx

Pengecekan nilai hash pada config.dbx menggunakan *tools* FTK Imager yang tertampil pada Gambar 4.9 yaitu memiliki nilai MD5 da8e3572c7a1110d8ff16afe4c67151c dan nilai SHA1 92be8f5ebdc1de5243a8a26b51b581833283837d.



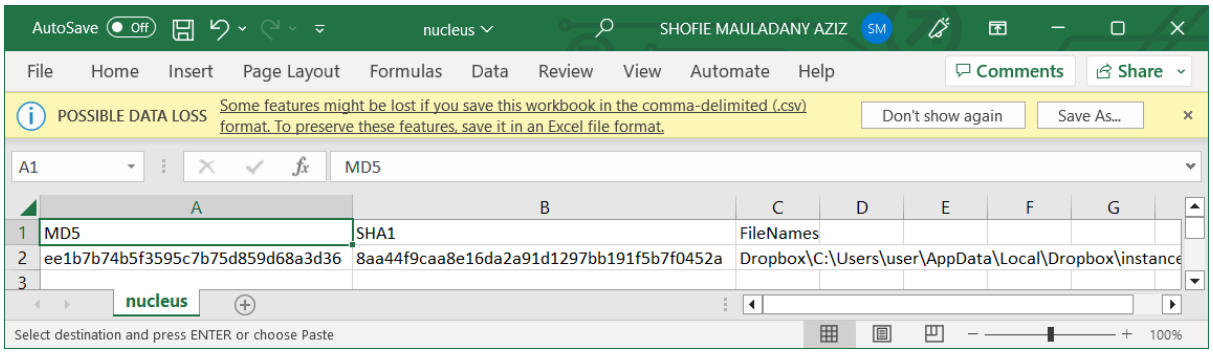
Gambar 4.10 Nilai Hash info.json

Pengecekan nilai hash pada info.json menggunakan *tools* FTK Imager yang tertampil pada Gambar 4.10 yaitu memiliki nilai MD5 5ccc863f69fc82e89b60bdc8d80a9a51 dan nilai SHA1 fa204c9856a932cc1990ee91df9b524a688f0efa.



Gambar 4.11 Nilai Hash sync_history.db

Pengecekan nilai hash pada sync_history.db menggunakan *tools* FTK Imager yang tertampil pada Gambar 4.11 yaitu memiliki nilai MD5 0830fb6eb770804b6d7a16fee8acbc0c dan nilai SHA1 0147ef08b8c5207f6bc55aec1b2ae52120e8f7dc.



Gambar 4.12 Nilai Hash nucleus.sqlite3

Pengecekan nilai hash pada file nucleus.sqlite3 menggunakan *tools* FTK Imager yang tertampil pada Gambar 4.12 yaitu memiliki nilai MD5 ee1b7b74b5f3595c7b75d859d68a3d36 dan nilai SHA1 8aa44f9caa8e16da2a91d1297bb191f5b7f0452a.

4.2.3 Analysis

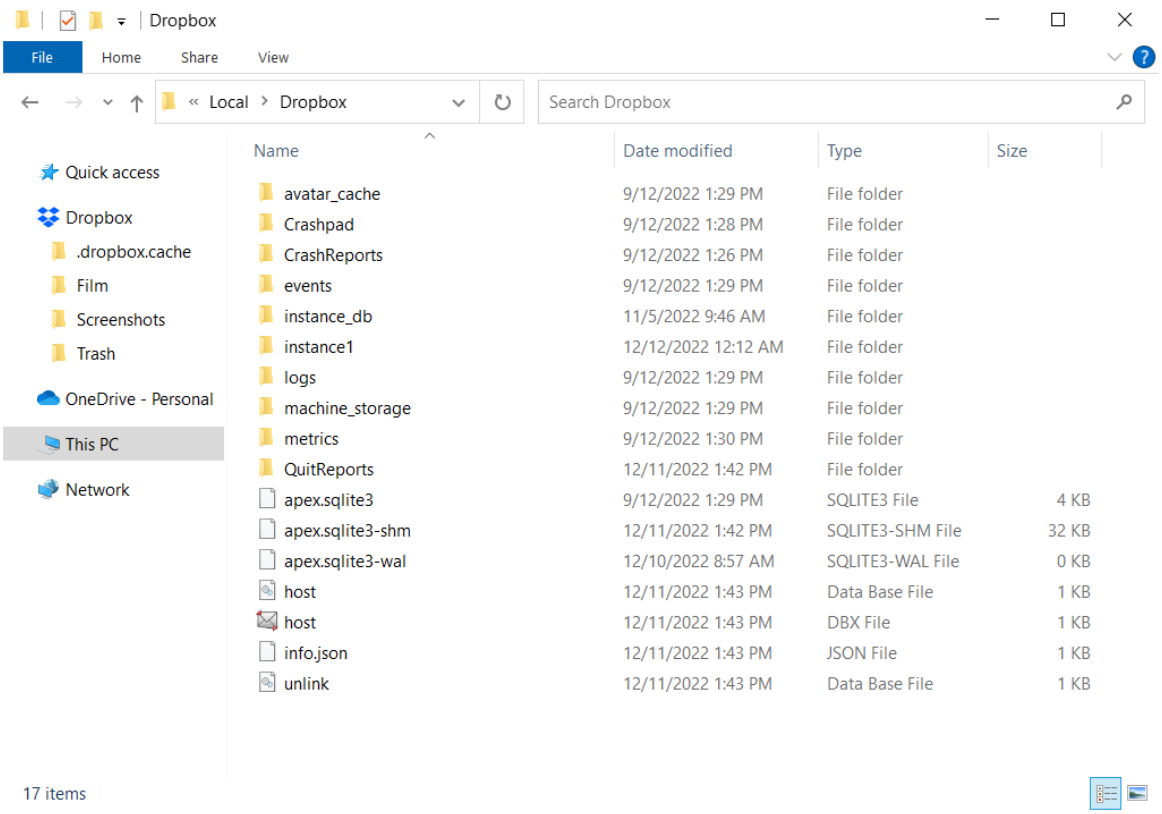
Dropbox yang telah terpasang pada perangkat akan otomatis membuat berbagai folder yang berfungsi untuk menyimpan segala sesuatu di dalam perangkat.

Tabel 4.4 Path File terkait Dropbox

File Path	Deskripsi
C:\Users\user\Dropbox	*Sync Folder* Dropbox pada Windows 10
C:\Users\user\Downloads\DropboxInstaller.exe	*Installer* yang telah di unduh
C:\Users\user\AppData\Roaming\Dropbox	Tidak dapat menentukan apa yang terdapat pada folder ini
C:\Program Files (x86)\Dropbox\Client	Dropbox Launcher
C:\Users\user\AppData\Local\Dropbox\instance1	Database Dropbox

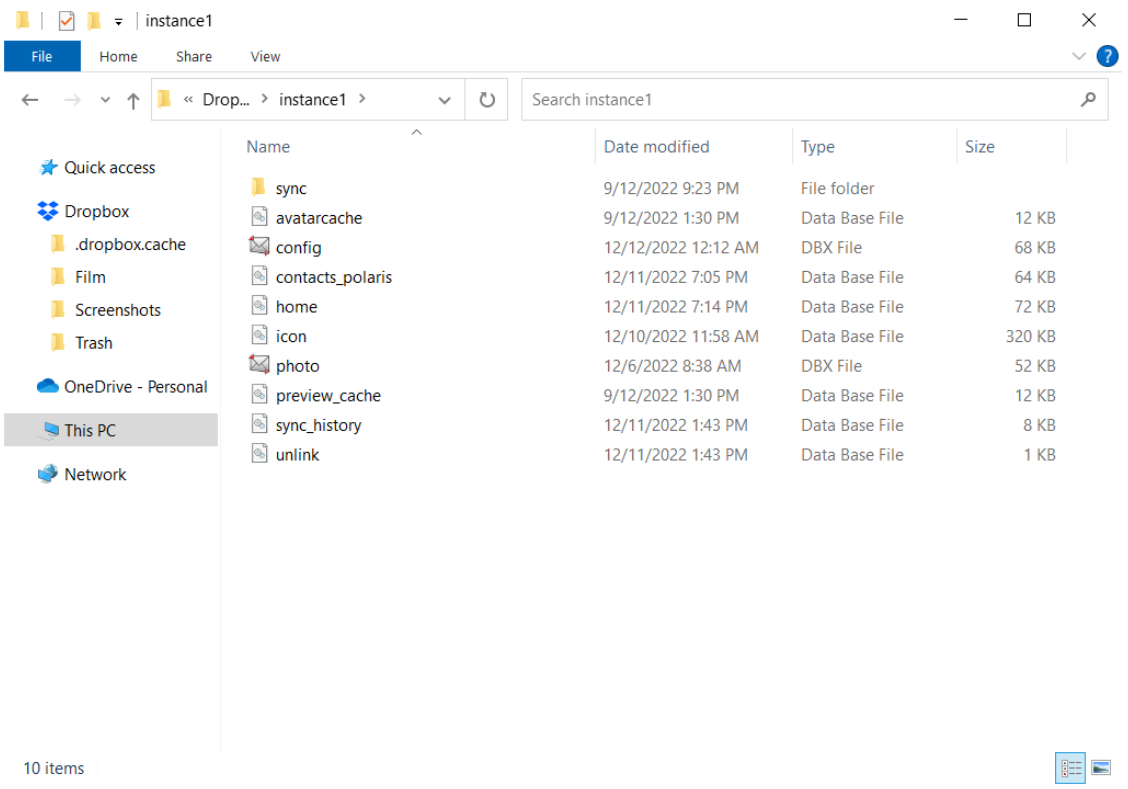
Berdasarkan Tabel 4.4 kita dapat mengetahui lokasi Dropbox sebelum di pasang dan sesudah di pasang pada perangkat. Direktori ini berguna untuk mencari apabila kita tidak mengetahui lokasi tersebut sebelumnya.

Setelah melakukan proses pemasangan aplikasi, langkah selanjutnya yaitu menganalisis data yang ada pada Dropbox. Data tersebut meliputi file.db pada Dropbox. Lokasi file.db pada Dropbox Desktop berada C:\Users\user\AppData\Local\Dropbox.



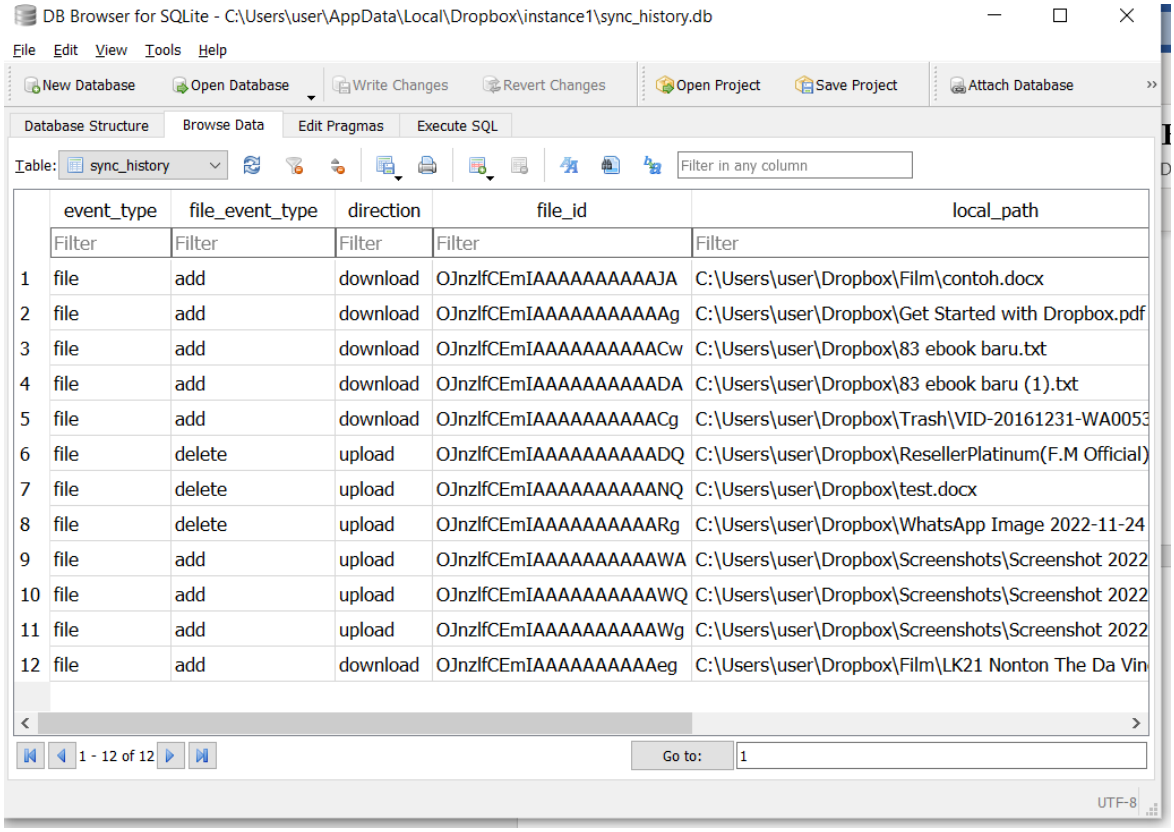
Gambar 4.13 Lokasi file.db berada

Pada Gambar 4.13 terlihat ada beberapa file database yang berisikan informasi terkait aktivitas yang dilakukan saat menggunakan aplikasi Dropbox. Folder ini berfungsi sebagai ‘otak’ dalam aplikasi Dropbox karena folder ini merupakan pusat kinerja pada aplikasi Dropbox. Pada C:\Users\user\AppData\Local\Dropbox terdapat file info.json yang berisikan file path, info tipe akun Dropbox dan juga info langganan Dropbox pada akun yang digunakan, dan terdapat dua file yang terenkripsi yaitu host.db dan host.dbx.



Gambar 4.14 Beberapa Database pada Dropbox

Pada Gambar 4.14 terlihat beberapa file database yang berisikan banyak informasi mengenai kegiatan yang dilakukan pada aplikasi Dropbox. File database ini yang kemudian akan dianalisis dan dijadikan laporan pada penulisan skripsi. Untuk dapat melihat isi dari database tersebut menggunakan tools yang telah disiapkan, akan tetapi database terenkripsi sehingga database tidak bisa diakses. Salah satu yang database yang terenkripsi yaitu config.dbx karena berisikan data pribadi pemilik akun Dropbox, adapun isi daripada database tersebut yaitu nama pengguna, alamat email pengguna, dan yang terakhir yaitu id host. Pada folder C:\Users\user\AppData\Local\Dropbox\instance1 terdapat sync_history.db yang berisikan riwayat sinkronisasi yang terjadi pada aplikasi Dropbox.



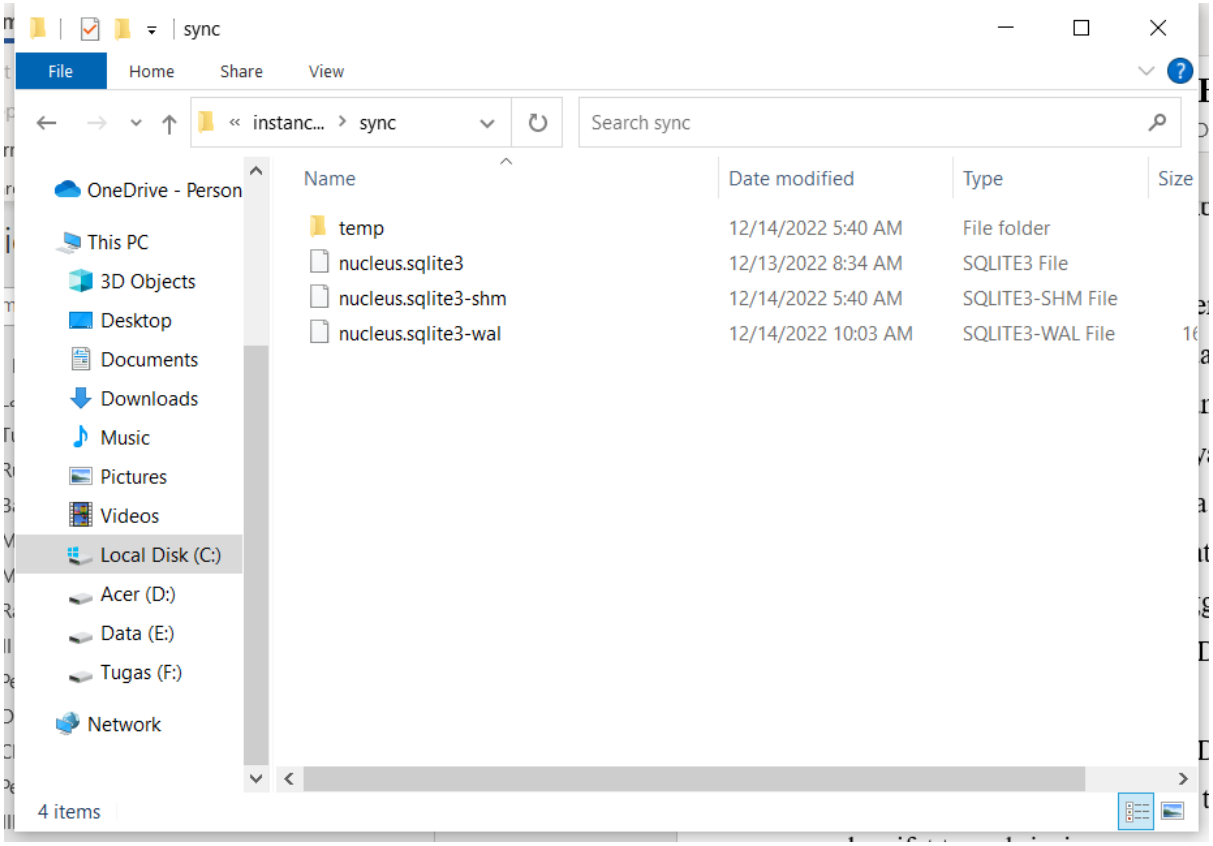
Gambar 4.15 sync_history.db

Gambar 4.15 merupakan file sync_history.db yang berisikan riwayat sinkronisasi file yang terjadi pada Dropbox Desktop, mulai dari aktivitas menambahkan atau mengupload file dan juga menghapus file. Dalam sync_history.db juga terdapat path file yang merupakan lokasi dimana file tersebut tersimpan di dalam perangkat komputer adapun rincian database sync_history.db tertulis dalam Tabel 4.5

Tabel 4.5 Rincian file sync_history.db

Variabel	Deskripsi
event_type	Bentuk file
file_event_type	Jenis aktivitas Tambahkan dan Hapus
Direction	Cara unggah file
file_id	ID file
local_path	Path file pada penyimpanan lokal
server_path	Path file pada server Dropbox

Kemudian pada folder C:\Users\user\AppData\Local\Dropbox\instance1\sync terdapat file database sql yang berisikan file apa saja yang tersimpan pada Dropbox dalam satu akun dan database ini bersifat terenkripsi.



Gambar 4.16 Folder ‘sync’ dalam instance1

4.2.4 Reporting

Tahap terakhir pada metode NIST ini menyajikan data yang telah diakuisisi dan dianalisis. Setiap data yang telah selesai dianalisis akan disajikan dalam bentuk tabel. Berikut adalah data yang telah berhasil diakuisisi.

Tabel 4.6 Data yang telah di akuisisi

Database	Path file
host.db	C:\Users\user\AppData\Local\Dropbox\host.db
host.dbx	C:\Users\user\AppData\Local\Dropbox\host.dbx
config.dbx	C:\Users\user\AppData\Local\Dropbox\instance1\config.dbx
info.json	C:\Users\user\AppData\Local\Dropbox\info.json
sync_history.db	C:\Users\user\AppData\Local\Dropbox\instance1\sync_history.db
nucleus.sqlite3	C:\Users\user\AppData\Local\Dropbox\instance1\sync\nucleus.sqlite3

LK21 Nonton The Da Vinci Code (2006) Film dan Series Streaming Download Movie Cinema21 Bioskop Subtitle Indonesia » Layarkaca21 HD Dunia21 IndoXXI [1].mp4	C:\Users\user\Dropbox\Film\LK21 Nonton The Da Vinci Code (2006) Film dan Series Streaming Download Movie Cinema21 Bioskop Subtitle Indonesia » Layarkaca21 HD Dunia21 IndoXXI [1].mp4

Laporan terkait nilai hash yang berhasil ditemukan menggunakan FTK Imager dan juga Magnet Forensik akan disajikan menggunakan tabel. Berikut adalah nilai hash dari setiap file yang telah di akuisisi sesuai pada Tabel 4.7.

Tabel 4.7 Nilai hash dari data yang telah di akuisisi

Nama File	**MD5**	**SHA1**
host.db	2ad2da74bbc9f7c85e417374b21b39d9	86331e527658f119cf8a999fc3fa2ceae7ad878f
host.dbx	36aa79a36e8bc468b72bdd5ec8f31953	df5b8c0a755eb41cfc5a18cf90b94672b61b6b03
config.dbx	da8e3572c7a1110d8ff16afe4c67151c	92be8f5ebdc1de5243a8a26b51b581833283837d
info.json	5ccc863f69fc82e89b60bdc8d80a9a51	fa204c9856a932cc1990ee91df9b524a688f0efa
sync_history.db	0830fb6eb770804b6d7a16fee8acbc0c	0147ef08b8c5207f6bc55aec1b2ae52120e8f7dc
nucleus.sqlite3	ee1b7b74b5f3595c7b75d859d68a3d36	8aa44f9caa8e16da2a91d1297bb191f5b7f0452a
LK21 Nonton The Da Vinci Code (2006) Film dan Series Streaming Download Movie Cinema21 Bioskop Subtitle Indonesia » Layarkaca21 HD Dunia21	ee50860decf5d5dbc3498f6c321683c5	b7dbb6d78ae527d7c7d5d40229d2d27d4389d114

IndoXXI [1].mp4		

Lokasi file yang terbentuk setelah proses instalasi selesai berhasil ditemukan dan akan disajikan dalam bentuk tabel.

Tabel 4.8 Path File terkait Dropbox

Path File	Deskripsi
C:\Users\user\Dropbox	*Sync Folder* Dropbox pada Windows 10
C:\Users\user\Downloads\DropboxInstaller.exe	*Installer* yang telah di unduh
C:\Users\user\AppData\Roaming\Dropbox	Tidak dapat menentukan apa yang terdapat pada folder ini
C:\Program Files (x86)\Dropbox\Client	Dropbox Launcher
C:\Users\user\AppData\Local\Dropbox\instance1	Database Dropbox

BAB V
KESIMPULAN

Berdasarkan hasil penelitian penggunaan metode NIST dalam proses *cloud forensic* dilakukan sesuai urutan pada NIST yaitu Collection, Examination, Analysis, dan Reporting. Tahap pertama berhasil mengumpulkan berbagai macam *tools* yang digunakan untuk membantu dalam proses analisis forensik. Pada proses examination berhasil melakukan pengecekan nilai hash dari setiap file yang telah diakuisisi yang menunjukan bahwa file tersebut merupakan file yang asli saat dilakukan pengakuisisian. Data yang ditemukan berupa file database pada aplikasi Dropbox dan juga film bajakan yang terdapat pada penyimpanan Dropbox. Data tersebut kemudian berhasil dianalisis dalam bentuk penetapan fungsi daripada setiap database yang ditemukan. Database yang dianalisis merupakan database penting pada aplikasi Dropbox Desktop. Dari seluruh database terdapat 6 database yang sangat penting diantaranya yaitu config.dbx, host.db, host.dbx, info.json, sync_history.db, dan nucleus.sqlite3, dan dari 6 database hanya 2 yang dapat diakses yaitu sync_history.db dan info.json dan 4 lainnya bersifat terenkripsi. Seluruh database yang dianalisis berhasil didapatkan nilai hash pada masing-masing file nya yang kemudian dijadikan bahan laporan pada penelitian. Saran untuk penelitian selanjutnya dapat melakukan dekripsi pada database yang terenkrip sehingga database dapat dianalisis lebih dalam dengan harapan menggunakan metode yang berbeda.

DAFTAR PUSTAKA

Aditya, A. D. P., Uning, P., & Syafridatati, S. (2021). *Penggunaan Digital Forensik Dalam Pengungkapan Kasus Penghinaan Di Internet (Studi Kasus Di Polda Sumatera Barat)*. http://repo.bunghatta.ac.id/6639/%0Ahttp://repo.bunghatta.ac.id/6639/3/Aditya Anggriawan Dwi Putra skripsi.pdf

Akbar, R., & Kudus, A. (2022). *Pelatihan Investigasi Digital Forensik*. *03*(02), 1–6.

APROFI, H. (2018). *Kampanye Anti Pembajakan Film*. sinemareview.com. https://www.sinemareview.com/2018/08/press-release-kampanye-anti-pembajakan.html

Aziz, D. (2022a). *Tangkapan Layar Film Bajakan Pada Akun Dropbox Milik Dany Aziz*. https://www.dropbox.com/home/Film

Aziz, D. (2022b). *Tangkapan layar Lk21*. lk21oficial.info

Berlian, Di. K. (2020). *Makin Penting, 8 Tips Gampang Amankan Data Pribadi*. Merdeka. https://www.merdeka.com/teknologi/makin-penting-8-tips-gampang-amankan-data-pribadi.html

Buyu, W., & Abade, E. O. (2020a). Forensic Analysis of Dropbox Data Remnants on Windows 10. *International Journal of Computer Applications*, *176*(41). https://doi.org/10.5120/ijca2020920546

Buyu, W., & Abade, E. O. (2020b). *Forensic Analysis of Dropbox Data Remnants on Windows 10 Forensic Analysis of Dropbox Data Remnants on Windows 10*. *July*. https://doi.org/10.5120/ijca2020920546

Dropbox. (2017). *Dropbox-Logo*. https://commons.wikimedia.org/wiki/File:Dropbox_logo_2017.svg

Dropbox. (2022). *Dropbox Plan*. Dropbox. https://www.dropbox.com/plans

Finance, B. (2022). *Mengenal Cyber Crime atau Kejahatan Digital Beserta Jenisnya*. Bfi.Co.Id. https://www.bfi.co.id/id/blog/mengenal-cyber-crime-atau-kejahatan-digital-beserta-jenisnya

Fisipol. (2022). *Penyebab Dan Dampak Dari Cyberbullying*. Universitas Medan Area Fakultas ISIPOL. https://ilmukomunikasi.uma.ac.id/2022/07/14/penyebab-dan-dampak-dari-cyberbullying/

Ko, A. C., & Zaw, W. T. (2015). Digital forensic investigation of dropbox cloud storage service. *Network Security and Communication Engineering - Proceedings of the 2014 International Conference on Network Security and Communication Engineering, NSCE 2014*, 147–150. https://doi.org/10.1201/b18660-32

Lasniroha, J. P., Juli, S., Ismail, I., Satrya, G. B., Telkom, U., & Digital, F. (2020a). *Mengidentifikasi Artefak Pada Aplikasi Dropbox Untuk Mendukung Forensic Android Identifying Artefact on Application Dropbox To Support Android*. *6*(2), 3293–3304.

Lasniroha, J. P., Juli, S., Ismail, I., Satrya, G. B., Telkom, U., & Digital, F. (2020b). *Mengidentifikasi Artefak Pada Aplikasi Dropbox Untuk Mendukung Forensic Android Identifying Artefact on Application Dropbox To Support Android*. *6*(2), 3293–3304.

Lim, S. Y., Johan, A., Daud, P., & Ismail, N. A. (2020). Dropbox forensics: Forensic analysis of a cloud storage service. *International Journal of Engineering Trends and Technology*, *1*, 45–49. https://doi.org/10.14445/22315381/CATI3P207

Mushlihudin, M., & Nofiyan, A. (2021). Analisis Forensik pada Web Phishing Menggunakan Metode National Institute of Standards and Technology. *Cybernetics*, *4*(02). https://doi.org/10.29406/cbn.v4i02.2287

Nasirudin, N., Sunardi, S., & Riadi, I. (2020). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89. https://doi.org/10.32493/informatika.v5i1.4578

Pandie, M. M., & Weismann, I. Th. J. (2016). Pengaruh Cyberbullying Di Media Sosial Terhadap Perilaku Reaktif Sebagai Pelaku Maupun Sebagai Korban Cyberbullying Pada Siswa Kristen SMP Nasional Makassar. *Jurnal Jaffray*, *14*(1), 43–62. https://doi.org/10.25278/jj.v14i1.188.43-62

Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics : Technical challenges , solutions and comparative analysis. *Digital Investigation*, *13*, 38–57. https://doi.org/10.1016/j.diin.2015.03.002

Putra, D. M. (2020). *4 Fakta Yogi Nara, Sosok "Perekam Ilegal" di Iklan Larangan Merekam di Bioskop*. Merdeka. https://www.merdeka.com/sumut/5-potret-yogi-nara-sosok-perekam-ilegal-di-iklan-larangan-merekam-di-bioskop.html

Ramadhan, B. (2021). *Dari mana sebuah situs mendapatkan film bajakan?* Quora.Id. https://id.quora.com/Dari-mana-sebuah-situs-mendapatkan-film-bajakan/answer/Budiman-Ramadhan/log

Ramadhan, R. A., Prayudi, Y., & Sugiantoro, B. (2017). Implementasi dan Analisis Forensika Digital Pada Fitur Trim Solid State Drive (SSD). *Teknomatika*, *9*(2), 1–13. http://teknomatika.stmikayani.ac.id/wp-content/uploads/2017/07/1.pdf

Riadi, I., Sunardi, & Sahiruddin. (2020). Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode Nist. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *7*(1), 197–204. https://doi.org/10.25126/jtiik.202071921

Riadi, I., Umar, R., & Nasrulloh, I. M. (2018). Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij). *Elinvo (Electronics, Informatics, and Vocational Education)*, *3*(1), 70–82. https://doi.org/10.21831/elinvo.v3i1.19308

Rochmanudin. (2019). *Diblokir Kemkominfo, Begini Pernyataan IndoXXI yang Kejutkan Warganet*. Indtimes. https://www.idntimes.com/news/indonesia/rochmanudin-wijaya/diblokir-kemkominfo-begini-pernyataan-indoxxi-yang-kejutkan-warganet?page=all

Rourke, M. (2020). *Cara Daftar Netflix Gratis dan Tanpa Kartu Kredit*. CNBCIndonesia. https://www.cnbcindonesia.com/tech/20200708130306-37-171130/cara-daftar-netflix-gratis-dan-tanpa-kartu-kredit

Saad, S. K., Umar, R., & Fadlil, A. (2020a). *Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas*. *4*(September), 293–299.

Saad, S. K., Umar, R., & Fadlil, A. (2020b). Analisis Forensik Aplikasi Dropbox Pada Android Menggunakan Metode NIST. *SEMINAR NASIONAL Dinamika Informatika 2020 Universitas PGRI Yogyakarta*, 119–123.

Satrya, G. B. (2019). *Digital Forensics Study of a Cloud Storage Client : A Dropbox Artifact Analysis*. *13*(2), 57–66.

Syahib, M. I., Riadi, I., & Umar, R. (2018). Analisis Forensik Digital Aplikasi Beetalk Untuk Penanganan Cybercrime Menggunakan Metode Nist. *Seminar Nasional Informatika 2018 (SemnasIF 2018)*, *1*(1), 134–139. http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2629/2207

Team Mendeley. (2012). Mendeley Logo Vertical. In *Flickr*. https://www.flickr.com/photos/33577340@N08/7603612464

Utami, N. R. (2022). *Menko PMK Sebut 45 Persen Anak di RI Jadi Korban C*. DetikNews. https://news.detik.com/berita/d-6039817/menko-pmk-sebut-45-persen-anak-di-ri-jadi-

korban-cyber-bullying#:~:text=Muhadjir menyebutkan 45 persen anak,(cyber bullying) sepanjang 2020

Vectors, F. L. (2022). *Scholar_Logo*. Pinterest. https://id.pinterest.com/pin/268456827778028382/

Yudhana, A., Riadi, I., & Anshori, I. (2018). *Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist*. *3*(1), 13–21.